ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 44, Number 5, 2014

REALIZING INFINITE CARDINAL NUMBERS VIA MAXIMAL CHAINS OF INTERMEDIATE FIELDS

DAVID E. DOBBS AND RAYMOND C. HEITMANN

To Roger Wiegand, on the occasion of his retirement

ABSTRACT. For each nonzero cardinal number κ, there is a field extension $\mathbf{Q} \subseteq L$ and a maximal chain $\mathcal{H}_\kappa$ of intermediate fields going from $\mathbf{Q}$ to L such that the cardinal number of $\mathcal{H}_\kappa$ is κ. If κ is infinite, then for all infinite cardinals $\nu < \kappa$, it can be arranged that $\mathcal{H}_\nu \subset \mathcal{H}_\kappa$. However, there exists an infinite cardinal for which there does not exist a field extension L/K such that κ is the supremum of the cardinalities of chains of intermediate fields going from K to L. For a field extension L/K, this supremum of cardinalities has been denoted $\lambda(L/K)$. If L/K is infinitely generated, we reduce its calculation to set theory, as follows. Let $\aleph_\alpha$ be the infimum of the cardinalities of generating sets of L/K. Let $\Omega(\aleph_\alpha)$ be the supremum of the cardinalities of chains of subsets of a set of cardinality $\aleph_\alpha$. ($\Omega(\aleph_\alpha)$ is equal to what has been called $\operatorname{ded}(\aleph_\alpha)$ in the literature.) Then $\aleph_\alpha < \Omega(\aleph_\alpha) \leq 2^{\aleph_\alpha}$; and if $\alpha > 0$ (but not necessarily if $\alpha = 0$), then $\lambda(L/K) = \Omega(\aleph_\alpha)$.

1. Introduction. In [**5**], Mullins and the first author introduced an invariant $\lambda(L/K)$ that gives an intuitive measure of the size of a field extension L/K. By definition, $\lambda(L/K)$ is the supremum (*qua* cardinal number) of the set of cardinal numbers that arise as lengths of chains of intermediate fields of L/K. (As usual, the *length* of a finite chain is defined as the number of "jumps" in it; to avoid possible ambiguity, we take the "length" of any infinite chain to be its cardinality.) Of course, an *intermediate field* of L/K is a field F such that $K \subseteq F \subseteq L$. It is

2010 AMS *Mathematics subject classification.* Primary 12F05, 12F20, 12F99, Secondary 13G05, 13A15.

Keywords and phrases. Field extension, intermediate field, chain, J-extension, cardinal number, transfinite induction, linear disjointness, integral domain, prime ideal.

The second author was partially supported by NSF grant DMS-0856124.

Received by the editors on January 11, 2012, and in revised form on June 5, 2012.

DOI:10.1216/RMJ-2014-44-5-1471

convenient to let $\mathcal{S}(L/K)$ denote the poset (under inclusion) consisting of the intermediate fields of L/K. In calculating $\lambda(L/K)$, one can restrict attention to chains $\mathcal{C}$ in $\mathcal{S}(L/K)$ that *go from* K *to* L, in the sense that $K, L \in \mathcal{C}$. Thanks to Zorn's lemma, one can also restrict attention to maximal such chains. Note also that if at least one chain in $\mathcal{S}(L/K)$ is infinite, then $\lambda(L/K)$ is also the supremum of the cardinalities of maximal chains in $\mathcal{S}(L/K)$ that go from K to L. As usual, it will be convenient to let $|T|$ denote the cardinal number of a set T.

It was shown in [**5**] that each finite cardinal number, as well as $\aleph_0$, can be realized as $\lambda(L/K)$ for some field extension L/K. The main result of that paper, [**5,** Theorem 3.2], addressed the case of larger infinite cardinal numbers and proved, assuming the Generalized Continuum Hypothesis (GCH), that if α is any infinite successor ordinal number, then $\aleph_\alpha$ can be realized as $\lambda(L/K)$ for some field extension L/K. Unfortunately, [**5,** Theorem 3.2] was stated incorrectly in [**5**], where the word "successor" was omitted from the statement of the result. The first author repeated that mistake when giving a talk on [**5**] several years ago at a meeting of the American Mathematical Society. When he returned to his seat after his talk, Roger Wiegand quietly and kindly asked him, "What about $\aleph_\omega$?". (As usual, ω denotes the smallest infinite ordinal number.) Indeed, [**5**] had failed to find *any* cardinal number of the form $\aleph_\alpha$, with α a limit ordinal number, that could be realized in the form $\lambda(L/K)$. The main purpose of this paper is to characterize $\lambda(L/K)$ for infinitely generated field extensions L/K, a byproduct being a negative answer to Wiegand's question.

We achieve the above "main purpose" assuming only ZFC; that is, the Zermelo-Fraenkel foundations for set theory, together with the Axiom of Choice. (This is what we mean in Section 4 when we give results that are valid "in any model".) As a result, we may use the usual rules for arithmetic with infinite cardinal numbers. Our current logical assumptions are to be contrasted with the approach in [**5**], which used the following consequence of GCH: if S is an infinite set, with $\aleph := |S|$, then there is a chain $\mathcal{C}$, consisting of subsets of S, such that $|\mathcal{C}| = 2^{\aleph}$. (A correct explanation of which set-theoretic principles imply the preceding assertion can be found in [**3,** Remark 2.2].) In the present paper, the *only* place where we assume GCH is Theorem 4.5 (a).

We begin with an elementary section that gives a positive answer to a weakened version of Wiegand's question. Theorem 2.2 shows how to realize any cardinal number κ, via a suitable field extension L/K, as the cardinality of some maximal chain H_κ in $\mathcal{S}(L/K)$ that goes from K to L. Theorem 2.2 goes further than [**4,** Example 2.5], where a similar conclusion had also been achieved, in the following way. The chains constructed in Theorem 2.2 are "compatible," in the sense that $H_\nu \subset H_\kappa$ for any infinite cardinals $\nu < \kappa$. Moreover, all of the H_κ in Theorem 2.2 have the same base field K. Also, we note that the classical $D + M$ construction is used in Corollary 2.4 to give the analogue of Theorem 2.2 for chains of commutative rings of positive Krull dimension.

The deeper work in this paper reduces the calculation of $\lambda(L/K)$, for an infinitely generated field extension L/K, to set theory. This main result is stated in Theorem 4.3. To prepare for this, we devote Section 3 to a study of generating sets of field extensions L/K. Suppose that L/K is infinitely generated. Then the infimum of the cardinalities of generating sets of L/K is some cardinal number $\aleph_\alpha$. It is shown in Corollary 3.3 that $\aleph_\alpha$ is the cardinality of any so-called "traditional generating set" of L/K. (The definitions of "traditional generating set" and the related concept of "special generating set" are given in Section 3.) We define $\Omega(\aleph_\alpha)$ to be the supremum of the cardinalities of chains that consist of subsets of a set of cardinality $\aleph_\alpha$. It turns out that $\aleph_\alpha < \Omega(\aleph_\alpha) \leq 2^{\aleph_\alpha}$ (Lemma 4.4). In that sense, the determination of $\Omega(\aleph_\alpha)$ is a matter of set theory. However, Theorem 4.3 and Proposition 4.2 combine to show that if $\alpha > 0$ (but not if $\alpha = 0$), then $\lambda(L/K) = \Omega(\aleph_\alpha)$. It follows in Theorem 4.5 (a) that if one also assumes GCH, then one can determine precisely which cardinal numbers are realizable as λ-values, and one thus has a negative answer to Wiegand's question. Moreover, Theorem 4.5 (b) identifies an infinite cardinal number which is not a λ-value in *any* model.

While the applications in Section 4 are stated rather early in Theorem 4.5 and the main result that justifies these applications is stated even earlier in Theorem 4.3, the bulk of Section 4 is devoted to the proof of Theorem 4.3, with Theorem 4.6 establishing that $\lambda(L/K) \leq \Omega(\aleph_\alpha)$ and Theorem 4.12 establishing (the harder fact) that $\lambda(L/K) \geq \Omega(\aleph_\alpha)$ if $\alpha > 0$. Following the proof of Theorem 4.5, the reader will find an extensive guide for explaining how the various pieces of the latter part of Section 4 fit together to establish these inequalities (and ultimately

Theorem 4.3). To reduce prerequisites for some to the technicalities in Section 4, material on linear disjointness is recalled and developed as needed.

In addition to the notation for cardinality mentioned above, we let $\subset$ and $\supset$ denote proper containments. For the appropriate background on cardinal numbers, ordinal numbers and transfinite induction, we recommend [**7**] and [**10**].

2. Realizing infinite cardinals via maximal chains of fields. Theorem 2.2 will give a sense in which every infinite cardinal number $\aleph_\alpha$ can be realized via a maximal chain of fields. In contrast to the proof in [**5,** Theorem 3.2] for the case where α is a successor ordinal, which made use of a certain algebraic field extension (and which used a consequence of GCH), the proof of Theorem 2.2 uses a purely transcendental field extension (and assumes only the usual ZFC foundations). Note that the proof of [**4,** Example 2.5] showed (without appeal to GCH) how to use the algebraic field extension from [**5,** Theorem 3.2] to build a maximal chain of fields that realizes any given $\aleph_\alpha$. However, our proof of Theorem 2.2 has the additional advantage that the base fields of these chains do not change as $\aleph_\alpha$ varies.

First, it will be convenient to use the next easy lemma to isolate a technique that will be used in the proof of Theorem 2.2. Although Lemma 2.1 will be applied to $\mathcal{S}(L/K)$, the proof is just as easy in a more general poset-theoretic context. If $(X, \leq)$ is a poset and $x_1 \leq x_2$ in X, then a "chain (respectively, maximal chain) in X going from x_1 to x_2" has the obvious meaning.

Lemma 2.1. *Let $(X, \leq)$ be a poset. If $\mathcal{C}_1$ (respectively, $\mathcal{C}_2$) is a maximal chain in X going from x_1 to x_2 (respectively, from x_2 to x_3), then $\mathcal{C} := \mathcal{C}_1 \cup \mathcal{C}_2$ is a maximal chain in X going from x_1 to x_3.*

Proof. It is clear that $\mathcal{C}$ is a chain in X going from x_1 to x_3, and so it remains only to prove maximality of $\mathcal{C}$. If the assertion fails, there exists $y \in X \setminus \mathcal{C}$ such that $x_1 \leq y \leq x_3$ and $\mathcal{D} := \mathcal{C} \cup \{y\}$ is also a chain (in X going from x_1 to x_3). Since $\mathcal{D}$ is a chain and $y \notin \mathcal{C}$, either $y < x_2$ or $x_2 < y$. If $y < x_2$, then $\mathcal{C}_1 \cup \{y\}$ is a chain in X going from x_1 to x_2, contradicting the maximality of $\mathcal{C}_1$. Similarly, $x_2 < y$ would lead to a contradiction of the maximality of $\mathcal{C}_2$. $\square$

We now present the main result of this section.

Theorem 2.2. *Let κ be any cardinal number. Then there exists a field extension $K \subseteq L$ (depending on κ) such that there is a maximal chain H_κ in $\mathcal{S}(L/K)$ that goes from K to L and satisfies $|H_\kappa| = \kappa + 1$. It can be arranged that $K = \mathbf{Q}$. If κ is infinite, then $K \subseteq L$ can furthermore be arranged so that $|L| = \kappa$. Moreover, it can also be arranged that $H_\nu \subset H_\kappa$ as chains in $\mathcal{S}(L/K)$ for all infinite cardinal numbers $\nu < \kappa$.*

Proof. We first take care of the case where κ is finite. Of course, $\lambda(K/K) = 0$ for any field K. Also, it is well known that if e is any positive integer and p is a prime number, then there exists an algebraic Galois field extension L of $\mathbf{Q}$ whose Galois group is cyclic of order p^e. Hence, by [**5,** Proposition 2.2 (a)], $\lambda(L/\mathbf{Q}) = e$. Thus, every whole number is realized as $\lambda(L/\mathbf{Q})$ for a suitable field L. This completes the verification in case κ is finite.

Next, we find a field extension $K_0 := \mathbf{Q} \subset L_0$ such that $\lambda(L_0/K_0) = \aleph_0$ as follows. Recall from [**6,** Theorem 3.9] that if K is a field that is neither algebraically closed nor real closed, then K has a J-extension L. (By definition, this means that L/K is an infinite-dimensional field extension such that $[F : K] < \infty$ for all fields F such that $K \subseteq F \subset L$.) In particular, $\mathbf{Q}$ has a J-extension L_0. It is known that if L/K is any J-extension (of fields), then $\lambda(L/K) = \aleph_0$ and, in fact, that each maximal chain in $\mathcal{S}(L/K)$ is denumerable (cf. [**4,** Proposition 2.7 (b)]). Also, it is well known (cf. [**8,** Lemma 3.5, page 259]) that if K is an infinite field and L is an algebraic field extension of K, then $|L| = |K|$. In particular, $|L_0| = \aleph_0$. This completes the verification in case $\kappa = \aleph_0$.

In the following, the symbols K_0 and L_0 retain the above meanings. Also, fix a (denumerable) maximal chain $\mathcal{C}$ in $\mathcal{S}(L_0/K_0)$ going from K_0 to L_0.

Next, suppose that $\kappa > \aleph_0$. Take X to be a well-ordered set, with no greatest member, that consists of (commuting) algebraically indeterminates over K_0 (i.e., over L_0). Put $L := L_0(X)$. By the usual laws of arithmetic for infinite cardinal numbers (which hold here since we have assumed ZFC), $|L| = |X| = \kappa$. For each $x \in X$, consider the subfield of L given by $F_x := L_0(\{y \in X \mid y < x\})$. We claim that the chain, which we call $\mathcal{D}_x$, given by

$$F_x \subset \cdots \subset F_x(x^{2^n}) \subset \cdots \subset F_x(x^4) \subset F_x(x^2) \subset F_x(x),$$

is a maximal chain of fields going from F_x to $F_x(x)$. Indeed, suppose, on the contrary, that there exists a field $F \in \mathcal{S}(F_x(x)/F_x) \setminus \mathcal{D}_x$ such that $\mathcal{D}_x \cup \{F\}$ is a chain. It is easy to see (via, for instance, [**9,** Theorem 7, page 158]) that $\cap_{n=0}^{\infty} F_x(x^{2^n}) = F_x$. Consequently, there exists a smallest whole number n such that $F \not\subseteq F_x(x^{2^n})$. Hence, $F_x(x^{2^n}) \subset F$. On the other hand, $n \geq 1$, and so the minimality of n leads to $F \subset F_x(x^{2^{n-1}})$. This contradicts the fact that $F_x(x^{2^{n-1}})/F_x(x^{2^n})$ is a two-dimensional (and hence minimal) field extension (cf. [**9,** Theorem 7, page 158]) and thus proves the above claim.

Consider any $y < z$ in X. Since $F_y(y) \subseteq F_z$, it follows easily that

$$\mathcal{D} := \{L_0, L\} \cup \ \cup_{x \in X} \mathcal{D}_x$$

is a chain in $\mathcal{S}(L/L_0)$ that goes from L_0 to L. Note that

$$\kappa = |X| \leq |\mathcal{D}| \leq \aleph_0 \cdot |X| = |X| = \kappa,$$

and so $|\mathcal{D}| = \kappa$. We claim that $\mathcal{D}$ is a maximal chain. Suppose, on the contrary, that there exists a field $F \in \mathcal{S}(L/L_0) \setminus \mathcal{D}$ such that $\mathcal{D} \cup \{F\}$ is a chain. Since $\cup_{x \in X} F_x = L$, it follows from the fact that X is well ordered that there exists a least $z \in X$ such that $F \not\supseteq F_z$. Hence, $F \subset F_z$ and $F \supseteq F_v$ for all $v < z$ in X. Without loss of generality, we can view X as an ordinal number, and so z is itself an ordinal number. Of course, $z \neq 0$, since $F \not\subset L_0 = F_0$. If z is a limit ordinal and $v < z$ in X, then $F_v \subseteq F \subset F_z$, which is a contradiction since the hypothesis on z ensures that $F_z = \cup_{v<z} F_v$. Therefore, z is a successor ordinal, with $z = z_0 + 1$ for some uniquely determined ordinal z_0. It follows that $F_{z_0} \subset F \subset F_z = F_{z_0+1} = F_{z_0}(z_0)$, which contradicts the maximality of $\mathcal{D}_{z_0}$. This proves the claim that $\mathcal{D}$ is a maximal chain.

The required chain is defined as $H_\kappa := \mathcal{C} \cup \mathcal{D}$. By Lemma 2.1, H_κ is a maximal chain in $\mathcal{S}(L/K_0)$ going from $K_0 = \mathbf{Q}$ to L. Evidently, $|H_\kappa| = |\mathcal{C}| + |\mathcal{D}| = \aleph_0 + \kappa = \kappa$. Finally, given an infinite cardinal number $\nu < \kappa$, note that there exist a well-ordered set (actually, an initial segment) $Y \subset X$ without a maximal element such that $|Y| = \nu$. Replacing X with Y in the above construction would produce a suitable chain H_ν. It is clear from the above construction that $H_\nu \subset H_\kappa$. □

We next collect some comments about the preceding result.

Remark 2.3. (a) The proof of Theorem 2.2 can be shortened. Indeed, after establishing the result for the case where κ is finite, one can handle the case of infinite κ by taking $L := \mathbf{Q}(X)$ and making the obvious modifications to the proof that was given above for the case $\kappa > \aleph_0$. In this way, one would have a proof of Theorem 2.2 which does not mention J-extensions and which does not need to appeal to Lemma 2.1. However, the above, longer, proof and Lemma 2.1 were included for the following reasons. First, J-extensions and the case $\kappa = \aleph_0$ will play a unique role early in Section 4: see the comment following the statement of Theorem 4.3. Second, when proving an assertion about infinite cardinals, it is often illuminating to give a proof for the case of $\aleph_0$ that is as concrete as possible.

(b) For infinite $\nu < \kappa$, perhaps the principal improvement that Theorem 2.2 provides when compared with [**4,** Example 2.5] is that the chains that were obtained above are "nested," in the sense that H_κ is simply an elongation of H_ν. This fact should not be obscured by the facts that we began with a specific (but arbitrary) κ and that we worked inside a specific field extension L/K while handling all the infinite cardinals ν that are less then or equal to κ. This formulation was used because the class of all the relevant ν then formed a set (and hence was susceptible to an argument involving well ordering).

Unfortunately, we cannot conclude that $\lambda(L/K) = \kappa$ in Theorem 2.2 for every infinite cardinal κ. The reason has nothing to do with the construction that was used in the above proof. Indeed, for each model with ZFC, some such κ is not a λ-value: see Theorem 4.5 below for this and for a complete answer to the motivating question of Roger Wiegand.

We close the section by pursuing a theme from [**5,** Corollary 3.8] and [**3,** Example 2.3], namely, by extending Theorem 2.2 to higher Krull dimensions. Recall that if D is an integral domain with quotient field F, then by an *overring* of D, we mean a ring E such that $D \subseteq E \subseteq F$. As usual, we take dim (R), the *Krull dimension* of a commutative unital ring R, to be the supremum of the lengths of chains of prime ideals of R, but when that supremum is infinite, we will view it as a cardinal number (not simply as ∞).

Corollary 2.4. *Let κ, d be nonzero cardinal numbers such that $\kappa \geq d+1$. Then there exists an integral domain R of Krull dimension d that has a maximal chain $\mathcal{C}^*$ of overrings going from R to its quotient field such that $|\mathcal{C}^*| = \kappa$.*

Proof. Let ν be a nonzero cardinal number satisfying $\nu + d = \kappa$. (The hypotheses on κ and d guarantee the existence of such ν. Note that ν is uniquely determined unless $\kappa = d$ is infinite, in which case any cardinal number $\nu \leq d$ can be used.) By Theorem 2.2, there exists a field extension $K \subseteq L$ and a maximal chain $\mathcal{C}$ of intermediate fields going from K to L such that $|\mathcal{C}| = \nu$. Next, let V be a valuation domain of Krull dimension d such that $V = L + M$, where M denotes the unique (nonzero) maximal ideal of V. Then the integral domain $R := K + M$ has the asserted properties. To see this, one uses the standard properties of the classical $D + M$ construction, as summarized in [**2,** Theorems 2.1 and 3.1]. First, one checks that $\mathcal{E} := \{A + M \mid A \in \mathcal{C}\}$ is a maximal chain of rings going from R to V. Next, recall from [**2,** Theorem 3.1] that each overring of R (inside the quotient field of R) is comparable with V under inclusion and, since V is a valuation domain, note that $\mathcal{F} := \{V_P \mid P \text{ is a nonmaximal prime ideal of } V\}$ is the unique maximal chain of proper overrings of V (inside the quotient field of R). Consequently, $\mathcal{C}^* := \mathcal{E} \cup \mathcal{F}$ is a maximal chain of overrings of R. Since this is a disjoint union, its cardinality is $|\mathcal{E}| + |\mathcal{F}| = |\mathcal{C}| + d = \nu + d = \kappa$. Finally, $\dim(R) = \dim(K) + \dim(V) = 0 + d = d$. □

Remark 2.5. (a) The restrictions on κ and d in Corollary 2.4 cannot be deleted. Indeed, if R is an integral domain having a chain of prime ideals $P_d \supset P_{d-1} \supset \cdots \supset P_0 = 0$ for some positive integer d and if $\mathcal{C}$ is any maximal chain of overrings of R (inside its quotient field) that contains $\{R_{P_i}\}$, then $|\mathcal{C}| \geq |\{R_{P_i}\}| = d + 1$.

(b) In view of Corollary 2.4 and (a), the referee has asked if a maximal chain of overrings of an integral domain R (inside the quotient field of R) must be of cardinality at least $\dim(R)$.

3. Special and traditional generating sets of a field extension. Let L/K be a field extension. It will be convenient to say that L/K is *infinitely generated* if there is no finite subset S of L such that $K(S) = L$. Of course, regardless of whether L/K is infinitely generated, this field extension does contain some generating sets, that is, sets S such that $K(S) = L$. In this brief section, we introduce two kinds of generating sets that are of particular interest when L/K is infinitely generated, namely, special generating sets (sgs) and traditional generating sets (tgs). The results given below show that if L/K is infinitely generated, then the study of its generating sets leads to an infinite cardinal number $\aleph_\alpha$ which depends only on L/K and which will be used in our main result, Theorem 4.3, to characterize $\lambda(L/K)$ whenever L/K is not countably generated.

Lemma 3.1 will be of particular use for algebraic field extensions, but the underlying definition can be given more generally. Let L/K be a field extension. Let W be any subset of L such that $K(W) = L$. We can view W as $\{w_\beta \mid \beta$ is an ordinal number such that $\beta < \alpha\}$ for some ordinal α. For each $\beta < \alpha$, let $W_\beta := \{w_\gamma \mid \gamma < \beta\}$, and let $I := \{\beta \mid w_\beta \notin K(W_\beta)\}$. Then let $Y := \{w_\beta \mid \beta \in I\}$ be indexed by the well-ordered set I. Any set Y that can be built in this way will be called an *sgs* (or *special generating set*) of L/K. Note that if an sgs Y of L/K is built via a set W such that $K(W) = L$, then Y satisfies $K(Y) = L$ (since there cannot exist a least element of W which is not in $K(Y)$).

It will be helpful, for any field extension L/K, to view $[L : K]$, the K-vector space dimension of L, as a cardinal number. In [**4,** Example 2.5], it was shown that if $\aleph_\alpha$ is any infinite cardinal number, then there exists an algebraic field extension L/K such that $[L : K] = \aleph_\alpha$.

Lemma 3.1. *Let L/K be a field extension. Then*:

(a) *If $L = K(W)$ for some set W, then there exists a special generating set Y of L/K such that $Y \subseteq W$. Thus, there exists a special generating set of L/K.*

(b) *Let Y be any special generating set of L/K. Then Y is linearly independent over K, and there exists a well-ordered chain $\mathcal{C}$ in $\mathcal{S}(L/K)$ which is order-isomorphic to Y and so $|\mathcal{C}| = |Y|$. If, in addition, L/K is infinite-dimensional and algebraic* (*that is, infinitely generated and algebraic*), *then $[L : K] = |Y|$.*

Proof.

(a) The first assertion was proved in discussing the above construction. The second assertion then follows from the case $W := L$ of the first assertion.

(b) If we had a linear dependence relation among the elements of Y, then each of those occurring with nonzero coefficient would be in the K-span of the others having nonzero coefficient. In particular, this would apply to the largest of the elements occurring with nonzero coefficient. But we know this element is not in the subfield of L generated over K by the smaller elements, let alone in their K-span. Since any linearly independent subset of a vector space can be extended to a basis, it follows that $|Y| \leq [L : K]$.

Next, we can construct the desired chain $\mathcal{C}$ as follows. For each $y \in Y$, consider the field $F_y := K(\{z \in Y \mid z \leq y\}) \in \mathcal{S}(L/K)$, where $\leq$ is the well ordering of some set W that led to the chosen construction of Y. It is clear that, if $y_1 \leq y_2$ in Y, then $F_{y_1} \subseteq F_{y_2}$. Moreover, if $y \in Y$, the construction of Y ensures that y is not a member of $\cup\{K(Y_z) \mid z \in Y, z < y\} = \cup\{F_z \mid z \in Y, z < y\}$. Therefore, the assignment $y \mapsto F_y$ sets up a bijection between Y and $\{F_y \mid y \in Y\}$, and so the latter set is a suitable $\mathcal{C}$. In particular, $\mathcal{C}$ inherits the property of being well ordered from (the indexing set I of) Y.

It remains to prove that $[L : K] \leq |Y|$ under the hypothesis that L/K is infinite-dimensional and algebraic. Note that this hypothesis guarantees that the sgs Y is infinite. If $y \in Y$, then the integer $n_y := [K(y) : K] \geq 2$ and $K(y) = \sum_{i=0}^{n_y - 1} Ky^i$. Consider the infinite set Σ of finite products defined by

$$\Sigma := \{y_1^{e_1} \cdots y_t^{e_t} \mid t \text{ a positive integer}, y_1, \dots, y_t \in Y, \\ 1 \leq e_i \leq n_{y_i} \quad \text{for each } i\}.$$

By algebraicity, $K(Y) = K[Y] = K + \sum_{z \in \Sigma} Kz$. Therefore, $\Sigma \cup \{1\}$ contains a K-basis of L, and so $[L : K] \leq |\Sigma|$. However, by the usual laws for arithmetic for infinite cardinal numbers (which hold since our riding assumptions include ZFC), $|\Sigma| = |Y|$. Thus, $[L : K] \leq |Y|$, to complete the proof. □

We next introduce a very useful kind of generating set of a field extension L/K. Let X be a transcendence basis of L/K, and let Y be a special generating set of $L/K(X)$. (The existence of such X is classical, and the final assertion of Lemma 3.1 (a) then gives the existence of such Y.) Note that $Z := X \cup Y$ is a generating set of the field extension L/K, since $K(Z) = K(X)(Y) = L$. Any such generating set Z of the above form will be called a *tgs* (or *traditional generating set*) of L/K. We next show that all the traditional generating sets of a given infinitely generated field extension have the same cardinality.

Proposition 3.2. *Let L/K be a field extension. Then*:

(a) *Let W be a subset of L such that $K(W) = L$. Then W contains a traditional generating set of L/K; that is, there exist a transcendence basis X of L/K and a special generating set Y of $L/K(X)$ such that $X \cup Y \subseteq W$.*

(b) *L/K has a traditional generating set.*

(c) *Suppose, in addition, that L/K is infinitely generated. Then any two traditional generating sets of L/K have the same cardinality*; *in other words, if X_1 and X_2 are transcendence bases of L/K with Y_1 a special generating set of $L/K(X_1)$ and Y_2 a special generating set of $L/K(X_2)$, then $|X_1 \cup Y_1| = |X_2 \cup Y_2|$.*

Proof.

(a) It is standard that W contains some transcendence basis X of L/K. Since $K(X)(W \setminus X) = L$, it follows from the first assertion in Lemma 3.1 (a) that $W \setminus X$ contains a special generating set Y of $L/K(X)$.

(b) Apply (a), with $W := L$.

(c) For $i = 1, 2$, let $Z_i := X_i \cup Y_i$. Since $X_i \cap Y_i = \emptyset$ and Z_i is infinite by the assumption on L/K, we have $|Z_i| = |X_i| + |Y_i| = \max(|X_i|, |Y_i|)$. Note also that $|X_1|$ and $|X_2|$ are equal, since each of these equals the transcendence degree of the extension L/K. Now, suppose that the assertion fails. Without loss of generality, $|Z_2| < |Z_1|$. We have $|X_1| = |X_2| \leq |Z_2| < |Z_1|$ and so $|Y_1| = |Z_1|$ is infinite. So by Lemma 3.1 (b), $[L : K(X_1)] = |Y_1| = |Z_1|$. Also, since $K(X_1 \cup Z_2) = L$, it follows from Lemma 3.1 (a) that the extension $L/K(X_1)$ has a special generating set Y such that $Y \subseteq Z_2$. Again, by Lemma 3.1 (b), $|Y| = [L : K(X_1)] = |Z_1|$. Then $|Z_1| = |Y| \leq |Z_2| < |Z_1|$, a contradiction, which completes the proof. □

The next result follows immediately from Proposition 3.2.

Corollary 3.3. *Let L/K be an infinitely generated field extension. Let $\aleph_\alpha$ be the infinite cardinal number which is the infimum of the cardinalities of generating sets of L/K. Then L/K has a traditional generating set of cardinality $\aleph_\alpha$, and each traditional generating set of L/K has cardinality $\aleph_\alpha$.*

It is easy to produce examples showing that the assertions in Proposition 3.2 (b) and Corollary 3.3 would fail if one deleted the hypothesis that the field extension L/K is infinitely generated. For instance, if an element x is transcendental over a field K, then $L := K(x)$ is a finitely generated field extension of K but L/K has traditional generating sets with unequal cardinalities: consider the tgs $X_1 \cup Y_1$ and $X_2 \cup Y_2$, where $X_1 := \{x^2\}, Y_1 := \{x\}, X_2 := \{x\}$ and $Y_2 := \emptyset$.

4. Not every infinite cardinal is a λ-value. In this section, we will reduce the computation of $\lambda(L/K)$ to strictly a problem in logic. The bulk of the section will be devoted to this reduction. Our results will allow us to show that the motivating question of Roger Wiegand has a negative answer and, in fact, allow us to give a complete picture of the situation when the generalized continuum hypothesis (GCH) holds. However, it should be noted that the main result in this section is independent of GCH. We begin with a definition.

Definition 4.1. Let $\aleph_\alpha$ be an infinite cardinal, U a set of cardinality $\aleph_\alpha$, and V the set of all chains that consist of subsets of U. Set $\Omega(\aleph_\alpha) := \sup\{|C| \mid C \in V\}$.

It seems reasonable that the actual value of $\Omega(\aleph_\alpha)$ depends upon the model we choose for our set theory. Although determining $\Omega(\aleph_\alpha)$ may not be an algebra question, the main result of this section shows that determining the value of $\Omega(\aleph_\alpha)$ is central to answering questions such as that of Roger Wiegand. We will state that main result as Theorem 4.3. First, we determine a significant value of $\Omega(\aleph_\alpha)$.

Proposition 4.2. $\Omega(\aleph_0) = 2^{\aleph_0}$.

Proof. For each real number r, consider the set $B_r := \{q \in \mathbf{Q} \mid q < r\}$. Since $\mathbf{Q}$ is order-dense in $\mathbf{R}$, it follows that if $r_1, r_2 \in \mathbf{R}$, then $r_1 < r_2$ if and only if $B_{r_1} \subset B_{r_2}$. Thus, $C := \{B_r \mid r \in \mathbf{R}\}$ is a chain of subsets of $\mathbf{Q}$ such that $|C| = |\mathbf{R}| = 2^{\aleph_0}$. As $\mathbf{Q}$ has cardinality $\aleph_0$, the assertion therefore follows from the definition of $\Omega(\aleph_\alpha)$ when $\alpha = 0$. □

It is not a coincidence that the proof of Proposition 4.2 is reminiscent of the construction of $\mathbf{R}$ via Dedekind cuts in $\mathbf{Q}$. In fact, for any infinite cardinal number $\kappa = \aleph_\alpha$, the concept that we have denoted by $\Omega(\aleph_\alpha)$ has appeared in the literature as follows (cf. [**1,** page 87]): $\operatorname{ded}(\kappa) := \sup\{\lambda \mid \text{there is a linear order of cardinal } \kappa \text{ with } \lambda \text{ Dedekind cuts}\}$. The interested reader can easily verify that $\Omega(\aleph_\alpha)$ and $\operatorname{ded}(\kappa)$ define the same quantity. Our form of the definition of $\Omega(\aleph_\alpha)$ seems more intuitively connected to the problem at hand, and so our methods will not emphasize Dedekind cuts.

For an infinitely generated field extension L/K, it will be convenient to say that L/K is *minimally generated by* $\aleph_\alpha$ *elements* to mean that $\aleph_\alpha$ is the infimum of the cardinalities of the generating sets of L/K. In this context, Corollary 3.3 showed that each tgs (traditional generating set) of L/K has cardinality $\aleph_\alpha$.

Theorem 4.3. *Let L/K be an infinitely generated field extension which is minimally generated by $\aleph_\alpha$ elements, for some ordinal number $\alpha > 0$. Then $\lambda(L/K) = \Omega(\aleph_\alpha)$ $(= \operatorname{ded}(\aleph_\alpha))$.*

We pause to explain why the case $\alpha = 0$ was excluded from the statement of Theorem 4.3. If L/K is a J-extension, then [**4,** Proposition 2.7] shows that L/K is minimally generated by $\aleph_0$ elements and $\lambda(L/K) = \aleph_0$. But we showed in Proposition 4.2 that $\Omega(\aleph_0) = 2^{\aleph_0}$ $(> \aleph_0)$.

Before proceeding to the proof of Theorem 4.3, we will show (in Theorem 4.5) how it answers our question. First, Lemma 4.4 gives some key bounds.

Lemma 4.4. *Let $\aleph_\alpha$ be any infinite cardinal. Then $\aleph_\alpha < \Omega(\aleph_\alpha) \leq 2^{\aleph_\alpha}$.*

Proof. Let U be a set of cardinality $\aleph_\alpha$ and V the set of all chains of subsets of U. Any element of V has its cardinality bounded above by the (cardinal) number of subsets of U, and so it is clear that $\Omega(\aleph_\alpha) \leq 2^{\aleph_\alpha}$. It remains only to prove the first inequality. Let $\aleph_\beta$ be the smallest cardinal such that $\aleph_\alpha < 2^{\aleph_\beta}$. Note that $\aleph_\beta \leq \aleph_\alpha$, and so $\beta \leq \alpha$. To complete the proof, it suffices to construct a chain in V of cardinality $2^{\aleph_\beta}$.

Let S be the smallest ordinal with cardinality $\aleph_\beta$, and let W be the set of all subsets of S which have a maximal element. For each $x \in S$, let W_x be the set of all subsets of S which have maximal element x. Then $|W| = \sum_{x\in S} |W_x| \leq |S| \cdot \sup\{|W_x| \mid x \in S\} \leq \aleph_\beta \cdot \aleph_\alpha = \aleph_\alpha$. (The preceding argument used the fact that each $|W_x| \leq \aleph_\alpha$. To see why this holds, note that x can be viewed as an ordinal γ such that $\gamma < \aleph_\beta$. As S can be identified with $\aleph_\beta$ as ordinal numbers, $|\gamma| < \aleph_\beta$, and so it follows from the minimality of S that $\aleph_\alpha \geq 2^{|\gamma|}$. On the other hand, $|W_x| \leq 2^{|\gamma|} \leq \aleph_\alpha$, as asserted.) Hence (since we can view $S \subseteq U$), it will suffice to find a chain of subsets of W which has cardinality $2^{\aleph_\beta}$.

Let T be the set of subsets of S. Notice that $W \subset T$. We first construct a chain of subsets of T which has cardinality $2^{\aleph_\beta}$. We can put a "lexicographic" order on T as follows. Suppose A, B are distinct elements of T. Let x be the least element in $(A \setminus B) \cup (B \setminus A)$. Then we say that $A < B$ precisely if $x \in B$. Finally, for each $A \in T$, let $D_A := \{H \in W \mid H \leq A\}$. Suppose $A < B$ in T. It is straightforward to check that $<$ is transitive, and so $D_A \subseteq D_B$. Consider the least element $x \in B \setminus A$. Let $H := B \cap \{y \in S \mid y \leq x\}$. Then $H \in W$ and $A < H \leq B$. In particular, $H \in D_B \setminus D_A$. Thus, $D_A \subset D_B$. Therefore, $\mathcal{C} := \{D_A \mid A \in T\}$ is a chain of cardinality $|T| = 2^{|S|} = 2^{\aleph_\beta}$. Since each $D_A \subseteq W$, $\mathcal{C}$ is the required chain. □

Although we found it useful to give a direct proof of Proposition 4.2, its conclusion also follows from Lemma 4.4. Indeed, if one takes $\alpha = 0$ in the proof of Lemma 4.4, that proof shows that $\beta = 0$ satisfies $2^{\aleph_\beta} \leq \Omega(\aleph_\alpha) \leq 2^{\aleph_\alpha}$, whence $\Omega(\aleph_0) = 2^{\aleph_0}$.

We next show that in any model of ZFC, some infinite cardinal is not obtained as a λ-value. Note that the proof of Theorem 4.5 depends on Theorems 4.3 and 4.6 (whose proofs will be completed later). Note also that since Roger Wiegand's motivating question was in the context of the approach in [**5**]; that question is completely answered by Theorem

4.5 (a). In regard to the hypotheses of that part of the next result, recall that $ZF + GCH$ implies the Axiom of Choice (cf. [**10,** Theorem 6.12.3, page 351]).

Theorem 4.5.

(a) *Assume that the generalized continuum hypothesis* (GCH) *holds* (*along with* ZFC). *Then an infinite cardinal number* $\aleph_\alpha$ *is achievable as* $\lambda(L/K)$ *for some field extension* L/K *if and only if either* $\alpha = 0$ *or* α *is a successor ordinal. In particular* (*given GCH*), $\aleph_\omega$ *is not a* λ*-value.*

(b) (*Without assuming* GCH). *If* $\alpha > 0$ *and* $\aleph_\alpha$ *is a cardinal number with the property that* $2^{\aleph_\beta} < \aleph_\alpha$ *whenever* $\beta < \alpha$, *then there does not exist a field extension* L/K *such that* $\lambda(L/K) = \aleph_\alpha$. *In particular, if* κ *denotes the supremum of the denumerable sequence of cardinals which starts with* $\aleph_0$, *and where each subsequent term is the cardinality of the power set of the term preceding it, then for any field extension* L/K, $\kappa \neq \lambda(L/K)$.

Proof.

(a) If we assume the generalized continuum hypothesis, there are no cardinals strictly between $\aleph_\alpha$ and $2^{\aleph_\alpha}$, and so Lemma 4.4 can be restated as $\Omega(\aleph_\alpha) = 2^{\aleph_\alpha}$. Recall from [**4,** Proposition 2.7 (b)] that $\aleph_0 = \lambda(L/K)$ for any J-extension L/K. Hence, by Theorem 4.3, the infinite cardinals other than $\aleph_0$ that are achievable as $\lambda(L/K)$ for some field extension L/K which is minimally generated by $\aleph_\gamma$ elements for some $\gamma > 0$ are precisely the values $2^{\aleph_\alpha} = \aleph_{\alpha+1}$, i.e., the successor cardinals. Moreover, if a field extension L/K is minimally generated by $\aleph_0$ elements, then $\lambda(L/K)$ must be either $\aleph_0$ or $\aleph_1$, since Theorem 4.6 and Proposition 4.2 combine to show that $\aleph_0 \leq \lambda(L/K) \leq \Omega(\aleph_0) = 2^{\aleph_0}$ ($= \aleph_1$ using GCH).

(b) In the general case (without assuming GCH), suppose the first assertion fails. Then there exists $\alpha > 0$ such that $\aleph_\alpha$ is a cardinal number with the property that $2^{\aleph_\beta} < \aleph_\alpha$ whenever $\beta < \alpha$, and $\aleph_\alpha = \lambda(L/K)$ for some field extension L/K that is minimally generated by $\aleph_\gamma$ elements for some $\gamma \geq 0$. Since $\aleph_\alpha > 2^{\aleph_0}$, we can use Theorem 4.6 and Proposition 4.2 as in part (a) to rule out the $\gamma = 0$ case. Then Theorem 4.3 gives $\aleph_\alpha = \Omega(\aleph_\gamma)$. As $\aleph_\alpha$ is a supremum, there exists an index β such that $\aleph_\gamma < \aleph_\beta < \aleph_\alpha$. Thus, by Lemma 4.4, $\Omega(\aleph_\gamma) \leq \Omega(\aleph_\beta) \leq 2^{\aleph_\beta} < \aleph_\alpha$. This contradiction proves the first assertion of (b). As for the second assertion, note that the cardinal κ described there (and for that matter, every cardinal that occurs as a limit cardinal under the GCH assumption) satisfies the hypothesis on $\aleph_\alpha$ specified in the first assertion of (b). □

We shall prove Theorem 4.3 by reducing it to two theorems, namely, Theorem 4.6 ($\lambda(L/K) \leq \Omega(\aleph_\alpha)$) and Theorem 4.12 ($\lambda(L/K) \geq \Omega(\aleph_\alpha)$). The proof of the first is reasonably straightforward, and we will get to it fairly quickly. However, the second is more difficult and will require a series of lemmas. The ideas behind the proof are relatively simple but are easily obscured by the details. So it is best to give an outline of the proof of Theorem 4.12 at this point.

Let $K \subseteq L$ be an infinitely-generated field extension, and let $\aleph_\alpha$ be the least cardinality of a generating set for L over K. To prove Theorem 4.12, it will suffice to show that if there exists a chain of cardinality $\aleph_\beta$ that consists of subsets of a set of cardinality $\aleph_\alpha$, then we can find a chain of intermediate fields of L/K with cardinality $\aleph_\beta$. We shall get this by showing something even stronger, namely

$(*)$ L contains a subset T of cardinality $\aleph_\alpha$ such that intermediate fields generated over K by distinct subsets of T are distinct.

Once we have $(*)$, we simply choose a chain of subsets of T of the desired cardinality and then this chain induces the desired chain of intermediate fields.

The proof of $(*)$ will be broken into several cases. If L/K has the largest transcendence degree possible under our hypothesis, namely $\aleph_\alpha$, then any transcendence basis for L/K can serve as the desired T. If L/K has smaller transcendence degree, we can reduce to the case where L/K is algebraic. In this case, we shall see (Lemma 4.10) that the proof is relatively easy if L is generated over K by a set of elements that are algebraic of bounded degrees.

If α is not the supremum of countably many smaller ordinals (i.e., if $\aleph_\alpha$ has uncountable cofinality), then among the members of an appropriate sort of generating set, some degree must occur $\aleph_\alpha$ times, and this will allow us to reduce to the above mentioned bounded-degree case (Lemma 4.11). The result is harder to show if α is the supremum of countably many smaller ordinals $d_1 < d_2 < \cdots$. In this situation, we prove (Lemma 4.9) that L contains a countable family of subfields which are linearly disjoint over a common subfield, and whose degrees over that subfield are, respectively, $\aleph_{d_1}, \aleph_{d_2}, \ldots$. Inductively applying our result to these subextensions, and letting T be the union of the resulting sets $T_1, T_2, \ldots$, we obtain $(*)$ in this case as well.

Now we are ready for the easier half of our main theorem.

Theorem 4.6. *Let L/K be an infinitely generated field extension. Let X be a transcendence basis of L/K, and let Y be a special generating set for the* (*algebraic*) *field extension $L/K(X)$. Suppose $|X \cup Y| = \aleph_\alpha$* (*which is the infinite cardinal such that L/K can be minimally generated by $\aleph_\alpha$ elements*). *Then $\lambda(L/K) \leq \Omega(\aleph_\alpha)$.*

Proof. Suppose the theorem is false. Then there exists a chain $\{F_i \mid i \in I\}$ in $\mathcal{S}(L/K)$ that has cardinality $\aleph_\beta > \Omega(\aleph_\alpha)$. It is harmless to suppose that $F_i \neq F_j$ whenever $i \neq j$. Let U be the set of finite subsets of X. It is easy to check that $|U| \leq \aleph_\alpha$. For each i, let $U_i := \{D \in U \mid D \text{ is algebraically independent over } F_i\}$. Observe that if $F_i \subset F_j$, then $U_i \supseteq U_j$. Thus, $\{U_i\}$ is a chain. Note that repetition is permitted; that is, it is possible that $U_i = U_j$ with $i \neq j$. For each subset U' of U, define $\rho(U') := |\{i \mid U_i = U'\}|$. Note that $\rho(U') \leq |I| = |\{F_i\}| = \aleph_\beta$ for each U'. Let $V := \{U' \mid \rho(U') > 0\}$. By the above observation, V is a chain in U. As $|U| \leq \aleph_\alpha$, it follows from the definition of $\Omega(-)$ that $|V| \leq \Omega(\aleph_\alpha)$.

Now $|I| = \sum_{U' \subseteq U} \rho(U') = \sum_{U' \in V} \rho(U')$. By using the definition of addition and multiplication of cardinal numbers, one can easily see that $|I| = \aleph_\beta \leq |V| \cdot \sup_{U'} \rho(U') \leq \Omega(\aleph_\alpha) \cdot \sup_{U'} \rho(U')$. Hence, $\sup(\rho(U')) \geq \aleph_\beta$ (by the assumption on $\aleph_\beta$). But the reverse inequality is trivial since each $\rho(U') \leq |I|$. Thus, $\sup(\rho(U')) = \aleph_\beta$. Hence, there exists at least one subset U' of U such that $\rho(U') > \Omega(\aleph_\alpha)$. Fix one such U'. Since the only property of $\aleph_\beta$ that we have used is that it is larger than $\Omega(\aleph_\alpha)$, we can assume, without loss of generality, that $\rho(U') = \aleph_\beta$.

Next, replace the chain $\{F_i\}$ with its subchain that consists of the fields for which $U_i = U'$. Since the new chain still has cardinality $\aleph_\beta$, it is harmless to continue denoting the new chain by $\{F_i\}$. Let $X' \subseteq X$ be a transcendence basis of the field extension L/F_i for some i. We claim that, in fact, $X' \subseteq X$ is a transcendence basis of L/F_j for every j. To see this, we first show X' is algebraically independent over F_j. If not, then some nonempty finite subset $D \subseteq X'$ is algebraically dependent over F_j. Then $D \notin U_j = U' = U_i$, and so D is algebraically dependent over F_i, contradicting the assumption that X' is a transcendence basis of L/F_i. This gives the asserted algebraic independence of X' over F_j. To finish the proof of the claim, we must also show that L is algebraic over $F_j(X')$. It suffices to prove that any $x \in X$ is algebraic over $F_j(X')$. (Indeed, it would then follow that $F_j(X)$ is algebraic over $F_j(X')$; and hence, since L is algebraic over $F_j(X)$, that L is algebraic over $F_j(X')$.) Now x is algebraic over $F_i(X')$, and so x is necessarily algebraic over $F_i(x_i, \dots, x_n)$ for some finite set of elements $x_i, \dots, x_n \in X'$. Then, we have $\{x_1, \dots, x_n\} \in U_i = U_j$ and $\{x, x_1, \dots, x_n\} \notin U_i = U_j$. This gives L algebraic over $F_j(X')$ and completes the proof of the above claim.

For each i, consider the field $E_i := F_i(X')$. We claim that if $F_i \subset F_j$, then $E_i \subset E_j$. It is clear that $E_i \subseteq E_j$. Thus, to prove the claim, it suffices to show that if $t \in F_j \setminus F_i$, then $t \notin E_i$. If $t \in E_i$ $(= F_i(X'))$, then $t \in F_i(W)$ for some finite subset W of X', so that $t = f(W)/g(W)$ for some nonzero polynomials $f, g \in F_i[W]$. Of course, f and g cannot both be constants (since $t \notin F_i$), and so, since W is nonempty, the equation $f(W) - tg(W) = 0$ contradicts the fact that X' is algebraically independent over F_j. This proves the above claim. Therefore, there is no harm in replacing the chain $\{F_i\}$ with $\{E_i\}$ (since $|\{E_i\}| = \aleph_\beta$). Thus, L/F_i is an algebraic extension for each i. In addition, setting $Z := X \cup Y$, we have $L = F_i(Z)$ for each i.

Let $Z^\star$ be the multiplicative submonoid of L that is generated by the elements of Z. It is easy to check that $|Z^\star| = \aleph_\alpha$. Since we have reduced to the case where L is algebraic over F_i, it is also easy to see that, for each i, $Z^\star$ is a spanning set for L viewed as a vector space over F_i. (We will use this fact in the final paragraph of this proof.) We will now use a process mimicking the one we used above for transcendence bases. Let U^* be the set of finite subsets of $Z^\star$. Clearly, $|U^*| = \aleph_\alpha$. For each i, let $U_i^* = \{D \in U^* \mid D \text{ is a linearly independent set over } F_i\}$. Observe that if $F_i \subset F_j$, then $U_i^* \supseteq U_j^*$. Thus, $\{U_i^*\}$ is a chain (with repetition permitted). For each subset W' of U^*, define $\rho(W') := |\{i \mid U_i^* = W'\}|$. Note that $\rho(W') \leq |I| = |\{F_i\}| = \aleph_\beta$ for each W'. Let $V^* := \{W' \mid \rho(W') > 0\}$. By the above observation, V^* is a chain in U^*. As $|U^*| = \aleph_\alpha$, it follows that $|V^*| \leq \Omega(\aleph_\alpha)$.

As before, we see that $|I| = \sum_{W' \subseteq U^*} \rho(W') = \sum_{W' \in V^*} \rho(W')$. By using the definition of addition and multiplication of cardinal numbers, one can easily see that $|I| = \aleph_\beta \leq |V^*| \cdot \sup_{W'} \rho(W') \leq \Omega(\aleph_\alpha) \cdot \sup_{W'} \rho(W')$. Therefore, $\sup(\rho(W')) \geq \aleph_\beta$ (by the assumption on $\aleph_\beta$). Thus, there exists at least one subset W' of U^* such that $\rho(W') > \Omega(\aleph_\alpha)$. Fix one such W'. Since $\Omega(\aleph_\alpha) > 1$, we can choose $F_i \subset F_j$ such that $U_i^* = W' = U_j^*$. Finally, as noted above, we may choose a subset B of $Z^\star$ which is a basis for L as a vector space over F_i. Since $U_i^* = U_j^*$, a finite subset of $Z^\star$ is linearly independent over F_i if and only if it is linearly independent over F_j. Hence, each finite subset of B is necessarily linearly independent over F_j. Consequently, B is also a basis for L over F_j.

Suppose $\xi \in F_j \setminus F_i$, and let $b \in B$. Then ξb is the unique way of expressing the element ξb of L as a linear combination of elements of B with coefficients in F_j. So, since $F_i \subset F_j$ and $\xi \notin F_i$, ξb cannot be in the F_i-vector space spanned by B, a contradiction which completes the proof. □

The rest of this section is devoted to proving Theorem 4.12. First, we need some background on linear disjointness. As in [**9,** pages 160–167], consider field extensions F/K and L/K, with F and L both contained in some field E, and let FL denote the K-subalgebra of E generated by $F \cup L$. (In our applications, F/K and L/K will be algebraic, in which case FL is also the subfield of E generated by $F \cup L$.) We say that F and L are *linearly disjoint* (*over* K) if the surjective K-algebra homomorphism $F \otimes_K L \to FL$, $\sum a_i \otimes b_i \mapsto \sum a_i b_i$ for all $a_i \in F$, $b_i \in L$, is an injection (that is, a K-algebra isomorphism). This notion of linear disjointness is equivalent to the following: each subset of F that is linearly independent over K must be linearly independent over L; and linear disjointness of F and L over K implies that $F \cap L = K$.

The following lemma collects some useful facts about linear disjointness that will be used in the proof of Lemma 4.9. Its part (a) has been noted before in [**9,** page 161], but we have not found a proof of it in the literature, and so we have included an elementary proof of it. Part (b) of Lemma 4.7 is well known (cf. [**9**, Lemma, page 162], [**8**, Theorem 2.4, page 319]).

Lemma 4.7.

(a) *Let F/K and L/K be field extensions, with F and L both contained in a common extension field. Then F and L are linearly disjoint over K if* (*and only if*) *some K-vector space basis of F is linearly independent over L.*

(b) *Given fields $A \subseteq D \subseteq L$ and $A \subseteq B \subset C \subseteq L$, then D and C are linearly disjoint over A if and only if the following two conditions hold: D and B are linearly disjoint over A and DB and C are linearly disjoint over B.*

(c) *Given algebraic field extensions $J_0 \subset J_i \subset L$ for $i = 1, 2, 3$ such that J_2 and J_3 are linearly disjoint over J_0 and also such that J_1 and J_2J_3 are linearly disjoint over J_0, then J_1J_2 and J_1J_3 are linearly disjoint over J_1.*

Proof. To prove (a), suppose that some K-vector space basis $\mathcal{B} = \{v_i \mid i \in I\}$ of F is linearly independent over L. It suffices to show that if $\xi \in F \otimes_K L$ is sent to 0 by the canonical surjective K-algebra homomorphism $\alpha : F \otimes_K L \to FL$, then $\xi = 0$. In view of the canonical isomorphisms $F \otimes_K L \cong (\oplus_{i\in I} Kv_i) \otimes_K L \cong \oplus_{i\in I}(Kv_i \otimes_K L) \cong \oplus_{i\in I}(K \otimes_K L) \cong \oplus_{i\in I} L$, we can write ξ uniquely in the form $\xi = \sum_{i\in I} v_i \otimes w_i$ where each $w_i \in L$ and w_i is 0 for all but finitely many $i \in I$. Since $0 = \alpha(\xi) = \sum_i v_i w_i$, the fact that $\mathcal{B}$ is linearly independent over L gives $w_i = 0$ for all $i \in I$, whence $\xi = 0$, as required.

We will prove (c) using the above tensor product criterion for linear disjointness, leaving an alternate proof that uses vector space bases to the interested reader. (Although (b) is standard, the reader will also easily find a proof of it that uses tensor products.) By the hypotheses of (c), the multiplication maps $f : J_2 \otimes_{J_0} J_3 \to J_2J_3$ and $g : J_1 \otimes_{J_0} J_2J_3 \to J_1(J_2J_3)$ are isomorphisms. The canonical homomorphism $J_1 \otimes_{J_0} J_2 \to J_1 \otimes_{J_0} J_2J_3$ is injective since J_1 is J_0-flat, and so the multiplication map $J_1 \otimes_{J_0} J_2 \to J_1J_2$ inherits injectivity from g. The same can be said for the multiplication map $J_1 \otimes_{J_0} J_3 \to J_1J_3$. In addition, $1 \otimes f$ is a isomorphism from $J_1 \otimes_{J_0} J_2 \otimes_{J_0} J_3$ to $J_1 \otimes_{J_0} J_2J_3$.

It follows that $J_1J_2 \otimes_{J_1} J_1J_3$ is isomorphic to

$$\begin{aligned}(J_1 \otimes_{J_0} J_2) \otimes_{J_1} (J_1 \otimes_{J_0} J_3) &\cong J_1 \otimes_{J_0} J_2 \otimes_{J_0} J_3\\ &\cong J_1 \otimes_{J_0} J_2J_3 \cong J_1(J_2J_3).\end{aligned}$$

It is straightforward to check that the resulting isomorphism is the multiplication map from $J_1J_2 \otimes_{J_1} J_1J_3$ to $J_1(J_2J_3) = (J_1J_2)(J_1J_3)$. □

Theorem 4.8. *Let $\alpha > 1$ be an ordinal number, and let F/E be an algebraic field extension such that $[F : E] = \aleph_\alpha$. Consider any ordinal number $d < \alpha$. Then there exist fields $E_d, L_d, F_d \in \mathcal{S}(F/E)$ such that $E \subseteq E_d \subset L_d \subseteq F$ and $E_d \subset F_d \subseteq F$ satisfying*:

(i) *F_d and L_d are linearly disjoint over E_d*;
(ii) *$[L_d : E_d] = \aleph_d$; and*
(iii) *$[F_d : E_d] = \aleph_\alpha$.*

Proof. Choose an sgs T of the field extension F/E. By the earlier construction of such sets, T is a well-ordered set, $F = E(T)$, and adjoining any element $\tau \in T$ to the field generated by E and the set of predecessors of τ in T gives a proper field extension. Regarding each cardinal as the least ordinal with its cardinality, and hence, in particular, as a well-ordered set, we can give $\aleph_1 \times \aleph_d$ lexicographic order (under which $(\gamma, \delta) \le (\gamma', \delta')$ if and only if either $\gamma < \gamma'$ or both $\gamma = \gamma'$ and $\delta \le \delta'$), and note that it is then a well-ordered set of cardinality $< \aleph_\alpha$. Hence, by standard properties of well-ordered sets, it is order-isomorphic to a unique initial segment of T, say, by a map sending $(\gamma, \delta) \in \aleph_1 \times \aleph_d$ to $t_{\gamma,\delta} \in T$. Now, for each $\gamma \in \aleph_1$, let $S_\gamma := \{t_{\gamma,\delta} \mid \delta \in \aleph_d\}$. The restriction of the above map gives an order-isomorphism $\{\gamma\} \times \aleph_d \to S_\gamma$, and so $\aleph_d \cong S_\gamma$. Also, for each $\gamma \in \aleph_1$, consider the field $E_\gamma := E(\bigcup_{\beta<\gamma} S_\beta) \in \mathcal{S}(F/E)$. If $\beta < \gamma$ in $\aleph_1$, it follows easily that $E_\beta \subset E_\gamma$.

By Lemma 3.1 (b), $|T| = \aleph_\alpha$. As $\cup_{\gamma\in\aleph_1} S_\gamma$ has cardinality $< \aleph_\alpha$, $T' := T \setminus \cup S_\gamma$ must have cardinality $\aleph_\alpha$. Next, for each $\gamma \in \aleph_1$ and $t \in T'$, consider the field $E_{\gamma t} := E_\gamma(\{t' \in T' \mid t' < t\})$. Then, for each $\gamma \in \aleph_1$, we define the function $f_\gamma : T' \to \mathbf{Z}$ by $f_\gamma(t) := [E_{\gamma t}(t) : E_{\gamma t}]$ for each $t \in T'$. If $\beta < \gamma$ in $\aleph_1$, it is clear that $E_{\beta t} \subseteq E_{\gamma t}$, and so $f_\gamma(t) \le f_\beta(t)$ for each $t \in T'$. Since a strictly decreasing infinite sequence of positive integers cannot exist, it follows that, for each $t \in T'$, only finitely many $\gamma \in \Gamma$ exist such that $f_{\gamma+1}(t) < f_\gamma(t)$.

For each $\gamma \in \aleph_1$ and $t \in T'$, t satisfies a unique monic irreducible polynomial; let us call it $g_{t\gamma}(X)$, in $E_{\gamma t}[X]$. In other words, $g_{t\gamma}$ is the minimum polynomial of t over $E_{\gamma t}$. Thus, whenever $\beta < \gamma$ in $\aleph_1$, $g_{t\gamma}$ divides $g_{t\beta}$ in $E_{\gamma t}[X]$. This forces these polynomials to coincide when they have equal degrees, and so, for each $t \in T'$, the set $C_t := \{g_{t\gamma} \mid \gamma \in \aleph_1\}$ is finite. For each $g_{t\gamma} \in C_t$, choose the minimum relevant γ and then fix any finite subset $U_{t\gamma}$ of $\{t' \in T' \mid t' < t\}$ such that all of the coefficients of $g_{t\gamma}$ lie in the field $E_\gamma(U_{t\gamma})$. For each $t \in T'$, consider the finite set $U_t := \cup\{U_{t\gamma} \mid g_{t\gamma} \in C_t\}$.

Define $\preceq$ to be the smallest transitive and reflexive binary relation on T' such that $t_1 \in U_t$ implies $t_1 \preceq t$. We claim that, for each $t \in T'$, the set $V_t := \{t' \in T' \mid t' \preceq t\}$ is finite. Suppose that the claim is false. Then, since T' is well-ordered, there exists a unique least $t \in T'$ such that V_t is infinite. On the other hand, U_t is a finite subset of V_t. Moreover, it follows from the nature of the transitive and reflexive closure of a binary relation that $V_t = \{t\} \cup \bigcup\{V_{t'} \mid t' \in U_t\}$. If $t' \in U_t$, the minimality of t ensures that $V_{t'}$ is finite. The upshot is that V_t is finite, the desired contradiction, thus proving the above claim.

For all $\gamma \in \aleph_1$, let $W_\gamma := \{t \in T' \mid f_{\gamma+1}(t') < f_\gamma(t')$ for some $t' \in V_t\}$. By the above comments, for each $t \in T'$, only finitely many γ exist such that $t \in W_\gamma$. We claim that $\gamma \in \aleph_1$ exists such that $T' \setminus W_\gamma$ has cardinality $\aleph_\alpha$. Suppose that this claim is false. Then, for each $\gamma \in \aleph_1$, there exists a smallest ordinal number $m_\gamma < \alpha$ such that $|T' \setminus W_\gamma| \leq \aleph_{m_\gamma}$. (Of course, we necessarily have equality unless $m_\gamma = 0$.) Let $\Delta := \{m_\gamma \mid \gamma \in \aleph_1\}$. For each $m \in \Delta$, let $h(m) := |\{\gamma \in \aleph_1 \mid m_\gamma = m\}|$. Then $\aleph_1 = |\aleph_1| = \sum_{m \in \Delta} h(m) \leq |\Delta| \cdot \sup\{h(m) \mid m \in \Delta\}$. It follows that either $|\Delta| = \aleph_1$ or there exists $m \in \Delta$ with $h(m) = \aleph_1$. In the former case, we choose some $m \in \Delta$ with infinitely many predecessors in Δ, while in the latter case, we choose m so that $h(m) = \aleph_1$. In either case, $|T' \setminus W_\gamma| \leq \aleph_m$ for infinitely many $\gamma \in \aleph_1$; and, of course, $m < \alpha$. Let Σ denote the infinite subset of $\aleph_1$ that consists of all such γ. As γ runs through Σ, the union of this collection of sets of the form $T' \setminus W_\gamma$ has cardinality at most $|\aleph_1| \cdot \aleph_m = \aleph_{\max(1,m)} < \aleph_\alpha = |T'|$, and so this union must be a proper subset of T'. Therefore, $\cap_{\gamma \in \Sigma} W_\gamma$ is nonempty, a contradiction (since Σ is infinite). This proves the above claim.

Hereafter, we fix γ such that $|T' \setminus W_\gamma| = \aleph_\alpha$. We will show that $E_d := E_\gamma$, $L_d := E_{\gamma+1}$ and $F_d := E_d(T' \setminus W_\gamma)$ have the asserted properties. By the construction of T, we can transfinitely adjoin each element of $T' \setminus W_\gamma$ successively to E_d, getting a proper field extension at each step. As in the proof of Lemma 3.1 (b), it follows from algebraicity that $[F_d : E_d] = |T' \setminus W_\gamma| = \aleph_\alpha$, thus proving (iii). Similarly, since $L_d = E_\gamma(S_\gamma)$, we see that $[L_d : E_d] = |S_\gamma| = \aleph_d$, thus proving (ii). It remains only to prove (i).

First, we claim that if $t \in T' \setminus W_\gamma$, then $U_t \subseteq T' \setminus W_\gamma$. If the claim fails, pick $s \in U_t \cap W_\gamma$. Since $s \in W_\gamma$, some $t' \in V_s$ satisfies $f_{\gamma+1}(t) < f_\gamma(t)$. However, since $s \in U_t$, we have $s \preceq t$, and so $V_s \subseteq V_t$ since $\preceq$ is transitive. Thus, $t' \in V_t$, and so $t \in W_\gamma$, a contradiction, thus proving the claim.

For $\sigma \in \{\gamma, \gamma + 1\}$, consider $F_\sigma := E_\sigma(T' \setminus W_\gamma)$. Then $F_\gamma = F_d = E_\gamma(T' \setminus W_\gamma)$ and $F_{\gamma+1} = L_d(T' \setminus W_\gamma) = L_d F_d$. In each of the field extensions F_γ/E_γ and $F_{\gamma+1}/E_{\gamma+1}$, the larger field can be obtained from the smaller field by transfinitely/successively adjoining the individual elements of $T' \setminus W_\gamma$. Such adjunctions lead, in a natural way, to vector space bases of the larger field over the smaller field. By Lemma 4.7 (a), it suffices to prove that the natural E_γ-basis of F_γ is also linearly independent over $E_{\gamma+1}$. This, in turn, holds if $[E^*_{\gamma t}(t) : E^*_{\gamma t}] = [E^*_{\gamma+1,t}(t) : E^*_{\gamma+1,t}]$ for every $t \in T' \setminus W_\gamma$, where for $\sigma \in \{\gamma, \gamma+1\}$, we define $E^*_{\sigma t} := E_\sigma(\{t' \in T' \setminus W_\gamma \mid t' < t\})$. Now, since $E_{\sigma t} \supseteq E^*_{\sigma t}$, it is clear that

$$[E^*_{\sigma t}(t) : E^*_{\sigma t}] \geq [E_{\sigma t}(t) : E_{\sigma t}] = \deg(g_{t\sigma}) = f_\sigma(t).$$

However, for both of the possible values of σ, this inequality is an equality, since $g_{t\sigma} \in E^*_{\sigma t}[X]$, the point being that each coefficient of $g_{t\sigma}$ belongs to $E_\sigma(U_t)$ and (as we showed above) $U_t \subseteq T' \setminus W_\gamma$. Therefore, it suffices to prove that $f_{\gamma+1}(t) = f_\gamma(t)$. But this holds since $t \notin W_\gamma$. The proof is complete. □

Lemma 4.9. *Let α be an ordinal number for which there exists a denumerable ascending chain $d_1 < d_2 < \cdots$ of ordinal numbers such that* $\sup\{d_i\} = \alpha$. *Let L/K be an algebraic field extension such that $[L : K] = \aleph_\alpha$. Then there exist fields $K', M_1, M_2, M_3, \ldots \in \mathcal{S}(L/K)$ such that $K \subseteq K' \subset M_i \subseteq L$ for each positive integer i, satisfying*

(i) *if $i, k_1, \ldots, k_m$ are finitely many pairwise distinct positive integers, the field composite $\prod_{j=1}^m M_{k_j}$ and M_i are linearly disjoint* *over K';*

(ii) $[M_i : K'] = \aleph_{d_i}$ *for each positive integer i.*

Proof. For each $n \geq 1$, we will use an inductive procedure to define intermediate fields E_n, F_n, L_n. This will be done in such a way that, for all $n \geq 1$,

- $K \subseteq E_n \subset L_n \subseteq L$ and $E_n \subset F_n \subseteq L$;
- $E_n \supseteq E_{n-1}$ and $F_n \subseteq F_{n-1}$, with $E_0 := K$ and $F_0 := L$;
- $[L_n : E_n] = \aleph_{d_n}$ and $[F_n : E_n] = \aleph_\alpha$;
- $H_n := \prod_{i=1}^n L_i$ and F_n are linearly disjoint over E_n; and
- $(\prod_{1 \leq j < n} L_j)E_n$ and L_n are linearly disjoint over E_n.

For the induction basis, apply Lemma 4.8 to the case where $F = L$, $E = K$, and $d = d_1$. This gives us E_1, L_1 and F_1. By Lemma 4.8, these fields have all of the five bulleted properties for $n = 1$.

For the induction step, assume $E_n, F_n, L_1, \ldots, L_n$ have been chosen with the above properties. Apply Lemma 4.8 with $F = F_n$, $E = E_n$ and $d = d_{n+1}$. This gives us E_{n+1}, L_{n+1} and F_{n+1}. The first three bulleted items are immediate from Lemma 4.8 (when n is replaced by $n+1$). To verify the remaining two bulleted items (concerning linear disjointness), we will repeatedly make use of Lemma 4.7 (b).

By the induction assumptions, H_n and F_n are linearly disjoint over E_n. As $F_{n+1}L_{n+1} \subseteq F_n$, it follows that H_n and $F_{n+1}L_{n+1}$ are linearly disjoint over E_n. Hence, applying Lemma 4.7 (b), with $A = E_n, D = H_n, B = L_{n+1}$ and $C = F_{n+1}L_{n+1}$, we find that H_nL_{n+1} and $F_{n+1}L_{n+1}$ are linearly disjoint over L_{n+1}. Also, we know from Lemma 4.8 that L_{n+1} and F_{n+1} are linearly disjoint over E_{n+1}. Now $H_{n+1} = H_nL_{n+1} \supseteq E_{n+1}$. Hence, we can use the reverse direction of Lemma 4.7 (b), with $A = E_{n+1}, D = F_{n+1}, B = L_{n+1}$ and $C = H_nL_{n+1}$, to get that $H_{n+1} = H_nL_{n+1}$ and F_{n+1} are linearly disjoint over E_{n+1}. This completes the proof of the induction step for the fourth bulleted item.

We turn to the fifth bulleted item. By the induction hypothesis, H_n and F_n are linearly disjoint over E_n. Thus, H_n and L_{n+1} are linearly disjoint over E_n. Using Lemma 4.7 (b), with $A = E_n, B = E_{n+1}, C = L_{n+1}$ and $D = H_n$, we see that H_nE_{n+1} and L_{n+1} are linearly disjoint over E_{n+1}. This completes the proof by induction of all five bulleted items for all positive integers n.

Set $K' := \cup_{n=0}^{\infty} E_n$ and, for each positive integer i, set $M_i := L_i K'$. Clearly $K' \subseteq M_i$. Now fix i. Since $[L_i : E_i] = \aleph_{d_i}$ (by the third bulleted item), (ii) will follow if we find an isomorphism $M_i \cong K' \otimes_{E_i} L_i$ of vector spaces over K'. First, note that, for all integers $n \geq i$, $E_n \subseteq F_i$, yielding $K' \subseteq F_i$. So by the fourth bulleted item, K' and L_i are linearly disjoint over E_i; that is, the canonical multiplication map $K' \otimes_{E_i} L_i \to K' L_i = M_i$ is an isomorphism. This proves (ii).

We will prove (i) by contradiction. Suppose that m is minimal such that (i) fails, with $i, k_1, \dots, k_m$ appearing in a counterexample to (i). Let $n := \sup\{i, k_1, \dots, k_m\}$. We claim that $(\prod_{j=1}^{m} L_{k_j})E_n$ and $L_i E_n$ are linearly disjoint over E_n. Suppose this claim fails. In any event, the fifth bulleted item shows that the claim does hold if $n = i$, as $L_i E_n = L_n$ here. So, without loss of generality, $i < n$. Also, since the ordering of $k_1, \dots, k_m$ does not matter, we may assume $n = k_1$. Then, by another application of the fifth bulleted item, $L_i(\prod_{j=2}^{m} L_{k_j})E_n$ and L_n are linearly disjoint over E_n. Hence, by Lemma 4.7 (b), $L_i(\prod_{j=2}^{m} L_{k_j})E_n$ and $L_n(\prod_{j=2}^{m} L_{k_j})E_n$ are linearly disjoint over $(\prod_{j=2}^{m} L_{k_j})E_n$. In addition, by the minimality of m, $(\prod_{j=2}^{m} L_{k_j})E_n$ and $L_i E_n$ are linearly disjoint over E_n. (The preceding assertion can be justified as follows. By reasoning as above and using the minimality of m, we get $K' \otimes_{E_n} (\prod_{j=2}^{m} L_{k_j})E_n \cong \prod_{j=2}^{m} M_{k_j}$. Hence, any subset of $(\prod_{j=2}^{m} L_{k_j})E_n$ that is linearly independent over E_n must remain linearly independent over K'. However, since m is minimal, M_i and $\prod_{j=2}^{m} M_{k_j}$ are linearly disjoint over K'. Thus, any subset of $(\prod_{j=2}^{m} L_{k_j})E_n$ that is linearly independent over E_n must remain linearly independent over M_i and, a fortiori, linearly independent over $L_i E_n$.) Therefore, an application of the "if" part of Lemma 4.7 (b), with $A = E_n, D = L_i E_n, B = (\prod_{j=2}^{m} L_{k_j})E_n$ and $C = L_n(\prod_{j=2}^{m} L_{k_j})E_n$, shows that m cannot be part of a counterexample to the above claim. This proves the claim.

Because linear disjointness is a finitistic condition, the assumption that $\prod_{j=1}^{m} M_{k_j}$ and M_i are not linearly disjoint over K' means that there is a positive integer $d \geq n$ such that $(\prod_{j=1}^{m} L_{k_j})E_d$ and $L_i E_d$ are not linearly disjoint over E_d. (Since tensor product commutes with direct limit, the preceding assertion can also be seen via the tensor product view of linear disjointness.) Choose d minimal with this property. By the claim established above, $d > n$. Hence, by the minimality of d, we have that $(\prod_{j=1}^{m} L_{k_j})E_{d-1}$ and $L_i E_{d-1}$ are linearly disjoint over E_{d-1}. To prove (i), it suffices to show that this fact, in conjunction with the fact that $(\prod_{j=1}^{m} L_{k_j})E_d$ and $L_i E_d$ are not linearly disjoint over E_d, leads to a contradiction.

Since the above inductive construction ensures that $E_{\nu+1} \subseteq F_\nu$ whenever $\nu \geq 1$ and $d \geq 2$, we have $E_d \subseteq F_{d-1}$. Therefore, since H_{d-1} and F_{d-1} are linearly disjoint over E_{d-1}, it follows that $(\prod_{j=1}^{m} L_{k_j})L_i E_{d-1}$ and E_d are linearly disjoint over E_{d-1}. Next, apply Lemma 4.7 (c) to $J_0 := E_{d-1}$, $J_1 := E_d$, $J_2 := (\prod_{j=1}^{m} L_{k_j})E_{d-1}$ and $J_3 := L_i E_{d-1}$. The upshot is that $E_d \prod_{j=1}^{m} L_{k_j}$ and $E_d L_i$ are linearly disjoint over E_d, the desired contradiction. □

Lemma 4.10. *Suppose L/K is an algebraic field extension with $[L : K] = \aleph_d$, for some ordinal d, and let n be a positive integer. Suppose U is an* sgs *of L/K with the property that $[K(t) : K] \leq n$ for every $t \in U$. Then there exists an intermediate field F with $K \subseteq F \subseteq L$ such that $F = K(T)$ for some set T of cardinality $\aleph_d$ with the property that, for any subsets S_1 and S_2 of T, one has that $K(S_1) = K(S_2)$ (if and) only if $S_1 = S_2$.*

Proof. We prove the result by induction on n. The base step $n = 1$ is vacuously true. For the induction step, assume the lemma holds for $n - 1$. First, consider the special case where there is a subset V of U such that $[L : K(V)] = \aleph_d$ and $[K(V)(t) : K(V)] < n$ for every $t \in U$. Then, by the induction hypothesis, the extension $L/K(V)$ must satisfy the conclusion of the lemma. We thus find a subset $T \subseteq L$ of cardinality $\aleph_d$ with the property that, for any subsets S_1 and S_2 of T, one has that $K(V)(S_1) = K(V)(S_2)$ only if $S_1 = S_2$. Clearly then, $K(S_1) = K(S_2)$ only if $S_1 = S_2$, and so T is the desired set in the special case. Hereafter, we assume, without loss of generality, that no V exists with the above properties.

Next, we describe a transfinite recursive procedure that will construct a well-ordered subset T of U such that $|T| = \aleph_d$. This transfinite procedure can be indexed by a subset of the sgs (hence well-ordered set) U.

Choose the least element of T to be the least element $\tau \in U$ whose minimal polynomial over K has degree n. (Such an element must exist, for otherwise, the empty set would be a set V with the above properties.) Observe that $[L : K(\tau)] = \aleph_d$ (since $[K(\tau) : K] < \infty$). Now, let S be the subset of (the desired set) T that has been constructed up to some specific step of the transfinite process. If $[L : K(S)] < \aleph_d$, the process terminates, with $T = S$, as S is clearly an sgs of $K(S)/K$, with Lemma 3.1 (b) ensuring that $|S| = [K(S) : K] = \aleph_d$. Thus, without loss of generality, $[L : K(S)] = \aleph_d$. Because S cannot satisfy the properties of V specified in the special case, there must exist an element $t \in U$ whose minimal polynomial over $K(S)$ has degree n. Choose the least such element t to be the next element of T.

Now that T has been constructed, consider the field $F := K(T)$. It remains only to prove that if S_1 and S_2 are subsets of T such that $K(S_1) = K(S_2)$, then $S_1 = S_2$. First, note that if $t_1 \leq \cdots \leq t_k$ in T, then an easy induction on k shows that $[K(t_1, \ldots, t_k) : K)] = n^k$. (For this induction, it is helpful to recall that $[K(\tau) : K] = n$.) Suppose the assertion fails. We can, without loss of generality, choose $x \in S_1 \setminus S_2$. Then $x \in M := K(y_1, \ldots, y_m)$ for some $y_1 < \cdots < y_m$ in S_2. As $N := K(y_1, \cdots, y_m, x) = M$, we have $n^m = [M : K] = [N : K] = n^{m+1}$. Since $n > 1$, we have the desired contradiction. □

Lemma 4.11. *Let d be any nonzero ordinal number which is not the supremum of any countable set of smaller ordinals.* (*Any successor ordinal has this property.*) *Suppose L/K is an algebraic field extension with $[L : K] = \aleph_d$. Then there exists an intermediate field F with $K \subseteq F \subseteq L$ such that $F = K(T)$ for some set T of cardinality $\aleph_d$ with the property that, for any subsets S_1 and S_2 of T, one has that $K(S_1) = K(S_2)$* (*if and*) *only if $S_1 = S_2$.*

Proof. Define a function $f : L \to \mathbf{Z}$ as follows: for each $t \in L$, let $f(t)$ be the degree of the minimal polynomial satisfied by t over K. For each positive integer i, consider the set $W_i := \{t \in L \mid f(t) \leq i\}$ and the field $L_i := K(W_i)$. We claim that there exists n such that $[L_n : K] = \aleph_d$. Suppose the claim fails. Then each L_i has a K-basis $\mathcal{B}_i$ of cardinality at most $\aleph_{e_i}$ with $e_i < d$. Let $e := \sup\{e_i\}$. By hypothesis, $e < d$. As L is the union of the increasing chain $\{L_i\}$, we can suppose that $\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \mathcal{B}_3 \subseteq \cdots$, so that $\mathcal{B} := \cup_{i=1}^{\infty} \mathcal{B}_i$ is a K-basis of L.

Therefore,

$$\aleph_d = [L : K] = |\mathcal{B}| \leq \sum_{i=1}^{\infty} |\mathcal{B}_i| \leq \aleph_0 \cdot \aleph_e = \aleph_e < \aleph_d,$$

a contradiction. This proves the above claim.

Next, as in the construction that preceded Lemma 3.1, build a special generating set U of L_n/K such that $U \subseteq W_n$. Since $L_n \in \mathcal{S}(L/K)$, there is no harm in replacing L with L_n. Thus, we may assume, without loss of generality, that $L = K(U)$, where U is an sgs of L/K and each element of U has its minimal polynomial over K having degree at most n. The result now follows from Lemma 4.10. □

We next give the final step in proving Theorem 4.3. Note that the assertion in Theorem 4.12 would fail if $\alpha = 0$ (by Proposition 4.2). In fact, the proof of Theorem 4.12 will use Lemma 4.11, whose proof used the condition $\alpha > 0$.

Theorem 4.12. *Let L/K be an infinitely generated field extension. Let X be a transcendence basis of L/K, and let Y be a special generating set for the* (*algebraic*) *field extension $L/K(X)$. Suppose $|X \cup Y| = \aleph_\alpha$* (*which is the infinite cardinal such that L/K can be minimally generated by $\aleph_\alpha$ elements*) *for some $\alpha > 0$. Then $\lambda(L/K) \geq \Omega(\aleph_\alpha)$.*

Proof. As explained earlier, it suffices to show

$(*)$ L contains a subset T of cardinality $\aleph_\alpha$ such that intermediate fields generated over K by distinct subsets of T are distinct.

Then, by $(*)$, if there exists a chain with cardinality $\aleph_\beta$ that consists of subsets of a set of cardinality $\aleph_\alpha$, then there exists a chain with cardinality $\aleph_\beta$ that consists of subsets of T, and hence there exists a chain in $\mathcal{S}(L/K)$ which has cardinality $\aleph_\beta$. This proves the theorem and so it only remains to show $(*)$.

Since $|X \cup Y| = \aleph_\alpha$, either $|X| = \aleph_\alpha$ or $|Y| = \aleph_\alpha$. If $|X| = \aleph_\alpha$, we claim $T := X$ is the desired subset. For suppose S_1 and S_2 are distinct subsets of X. Without loss of generality, there exists $x \in S_1 \setminus S_2$. Then $x \in K(S_1)$. However, because the set X is algebraically independent, $S_2 \cup \{x\}$ is algebraically independent, and so $x \notin K(S_2)$. In the remaining case, $|Y| = \aleph_\alpha$. Then we claim that it suffices to prove

$(*)$ with K replaced by $K(X)$. For, if T is a subset of L such that intermediate fields generated over $K(X)$ by distinct subsets of T are distinct, then intermediate fields generated over K by distinct subsets of T will also be distinct. We have thus reduced to the case where L/K is an algebraic extension.

By the final assertion of Lemma 3.1 (b), $[L : K] = \aleph_\alpha$. If α is not the supremum of some denumerable set of smaller ordinals, $(*)$ holds by Lemma 4.11. So we can reduce to the case where α is the supremum of some denumerable set $d_1 < d_2 < \cdots$ of smaller ordinals. In this case, we will find fields $E \subset F$ in $\mathcal{S}(L/K)$ such that $[F : E] = \aleph_\alpha$ and $F = E(T)$ for some set T of cardinality $\aleph_\alpha$, with the property that, if S_1, S_2 are subsets of T, then $E(S_1) = E(S_2)$ if and only if $S_1 = S_2$. This will suffice to prove $(*)$ as, just as in the above reduction to the algebraic case, subsets of T that generate distinct intermediate fields over E will generate distinct intermediate fields over the smaller field K.

To find suitable E, F and T, first apply Lemma 4.9 to find fields $K' \subset M_i$ in $\mathcal{S}(L/K)$ such that $[M_i : K'] = \aleph_{d_i}$ for every positive integer i and the linear disjointness properties in condition (i) of Lemma 4.9 hold. For each positive integer i, we have $\aleph_{d_i} < \aleph_{d_{i+1}} = [M_{i+1} : K'] \leq [L : K'] \leq [L : K] = \aleph_\alpha$, and so $[L : K'] = \aleph_\alpha$. Then, by abuse of notation, we can replace K with K'. Having done so, we then take E to be K (that is, the former K'). We next explain how to find F and T.

We claim that, for each positive integer i, there exist a set $T_{d_i} \subseteq L$ with cardinality $\aleph_{d_i}$ and an intermediate field $H_{d_i} := K(T_{d_i}) \in \mathcal{S}(M_i/K)$ with the following property: if S_1 and S_2 are subsets of T_{d_i} such that $K(S_1) = K(S_2)$, then $S_1 = S_2$. (Observe that this implies that $[H_{d_i} : K] = \aleph_{d_i}$.) If d_i is not the supremum of a denumerable set of smaller ordinals, the claim follows by applying Lemma 4.11 to the field extension M_i/K. On the other hand, if d_i is such a supremum, the claim holds because there is no harm in supposing that α is the minimal counterexample. This proves the above claim.

Let F be the field composite $\prod_i H_{d_i}$, and let T be the set $\cup_i T_{d_i}$. It is clear that $F = K(T)$. For every positive integer i,

$$\aleph_{d_i} = |T_{d_i}| \leq |T| \leq \aleph_0 \cdot \sup_j |T_{d_j}| \leq \aleph_0 \cdot \aleph_\alpha = \aleph_\alpha,$$

and so $|T| = \aleph_\alpha$.

It remains to prove that, if S_1 and S_2 are subsets of T such that $K(S_1) = K(S_2)$, then $S_1 = S_2$. Hence, it suffices to show, for each positive integer i, that $K(S_1 \cap T_{d_i}) = K(S_2 \cap T_{d_i})$. (The point is that we would then have that $S_1 \cap T_{d_i} = S_2 \cap T_{d_i}$ for each i and would only need to note that each $S_j = \cup_i (S_j \cap T_{d_i})$.) To that end, it clearly suffices to prove that if S is any subset of T and i is any positive integer, then $K(S \cap T_{d_i}) = K(S) \cap H_{d_i}$. As $T_{d_i} \subseteq H_{d_i}$, one inclusion is clear. If the assertion fails, pick an element x of $K(S) \cap H_{d_i}$ which does not belong to $K(S \cap T_{d_i})$. Consider the field $N := \prod_{j \neq i} H_{d_j}$. The field composite of $K(S \cap T_{d_i})$ with N obviously contains $K(S)$, and so x is an element of this field composite. We will proceed to show that x is, in fact, not an element of this field composite.

Choose $\mathcal{B}$ to be a basis of $K(S \cap T_{d_i})$ as a vector space over K. Then $\mathcal{D} := \mathcal{B} \cup \{x\}$ is linearly independent over K. As $\mathcal{D} \subseteq M_i$, the linear disjointness established in Lemma 4.9 (i) shows that $\mathcal{D}$ is also linearly independent over the field $N := \prod_{j \neq i} H_{d_j}$. Using algebraicity, we can rewrite and properly embed the field composite $K(S \cap T_{d_i})N$ as

$$\begin{aligned}\Bigg(\sum_{y \in \mathcal{B}} Ky\Bigg)N = \sum_{y \in \mathcal{B}} Ny \subset \sum_{z \in \mathcal{D}} Nz \\ = \Bigg(\sum_{z \in \mathcal{B}} Kz\Bigg)N + Nx \\ = K(S \cap T_{d_i})N + Nx,\end{aligned}$$

whence $Nx \not\subseteq K(S \cap T_{d_i})N$ and $x \notin K(S \cap T_{d_i})N$, the desired contradiction. The proof is complete. □

Note added in proof. (September 17, 2014). The question raised in Remark 2.5 (b) has an affirmative answer in the finite-dimensional case; that is, if R is an integral domain with quotient field K such that $\dim(R) < \infty$ and $\mathcal{C}$ is a maximal chain of rings going from R to K, then $|\mathcal{C}| \geq \dim(R) + 1$. For a proof, suppose, on the contrary, that $\mathcal{C}$ is the chain $R = R_0 \subset R_1 \subset \cdots \subset R_n = K$ where $n + 1 < \dim(R) + 1$. Notice that $R_0 \subset R_1$ is a minimal ring extension, and apply the fact that if $A \subset B$ is a minimal ring extension, then $\dim(B) \leq \dim(A) \leq \dim(B) + 1$. Then $n < \dim(R) \leq \dim(R_1) + 1$. Iterating the argument, we get that $n < \dim(R_2) + 2 < \cdots < \dim(R_{n-1}) + (n-1)$, and so $1 < \dim(R_{n-1})$, contradicting the fact that R_{n-1} is a one-dimensional valuation domain.

However, the question raised in Remark 2.5 (b) has a negative answer when $\dim(R)$ is infinite. We next give an example of a denumerable integral domain D, with quotient field K, such that $\dim(D) = 2^{\aleph_0}$ and there is a maximal chain $\mathcal{C}$ of rings going from D to K with $|\mathcal{C}| = \aleph_0$. Let D be the ring of polynomials over $\mathbf{Q}$ in denumerably many indeterminates X_q, where the index q runs over the set of positive rational numbers. Using the usual arithmetic with infinite cardinal numbers (assuming only ZFC), we get that the cardinality of D is $\aleph_0$. To see that $\dim(D) = 2^{\aleph_0}$, consider the chain of prime ideals $\{P_r \mid r$ is a positive real number$\}$, where P_r is the ideal of D that is generated by $\{X_q \mid q$ is a positive rational number such that $q < r\}$.

To complete the proof, it suffices to find a maximal chain of rings going from $S := \mathbf{Q}[X_1, X_2, \ldots]$ to $L := \mathbf{Q}(X_1, X_2, \ldots)$ of cardinality $\aleph_0$. (Notice that $S \cong D$.) Consider the denumerable (non-maximal) chain $S \subset \mathbf{Q}(X_1)[X_2, X_3, \ldots] \subset \mathbf{Q}(X_1, X_2)[X_3, X_4, \ldots] \subset \ldots$, whose union is L. It suffices to prove that there exists a denumerable maximal chain inside each of the denumerably many steps of the above chain (for one could then go from S to L via a maximal chain obtained as a countable union of countable chains). Since we are working with countable UFDs, notice that within each of those steps one could insert a countable (non-maximal) chain that is obtained by successively adjoining the multiplicative inverse of each member of a set of associate-class representatives of irreducible elements. It seems reasonable to speculate that, by using unique factorization, it should be possible to complete the argument by showing that, within each of *those* countably many steps, one can insert a countable maximal chain of rings. We choose, instead, to complete the argument by establishing the following (slightly more general) result.

Lemma. *Let $X_1, X_2, \ldots$ be denumerably many algebraically independent indeterminates over $\mathbf{Q}$, and let $D := \mathbf{Q}(X_1, \ldots, X_k)[X_{k+1}, \ldots]$ for some integer $k \geq 0$. Let $E = D_S$ where S is a multiplicatively closed subset of $\mathbf{Q}(X_1, \ldots, X_k)[X_{k+1}]$, and let f be a prime element of $\mathbf{Q}(X_1, \ldots, X_k)[X_{k+1}]$. Then there is a countable maximal chain of rings between E and $E[1/f]$.*

Proof of Lemma. Let K denote the field $\mathbf{Q}(X_1, \ldots, X_k)$, let $x := X_{k+1}$, and let Y denote the infinite set of indeterminates $\{X_{k+2}, \ldots\}$. So $E = K[x, Y]_S$ where $S \subset K[x]$ and $f \in K[x]$. If Q denotes the prime ideal YE of E, then $Q + fE$ is a maximal ideal of E. It is also easy to see that there exists a maximal denumerable chain of Q-primary ideals $Q = Q_1 \supset Q_2 \supset Q_3 \supset \cdots$ of E whose intersection is (0). Before constructing the desired maximal chain of rings, we make a simple observation. If T is an intermediate ring, i.e., $E \subseteq T \subseteq E[1/f]$, then each element of T has the form a/f^i for some $a \in E$ and $i \in N$. Moreover, $a/f^i \in T$ if and only if $a \in f^i T \cap E$. Thus, T is completely described by the set of ideals $J_i := f^i T \cap E$.

Define $R_{mn} := E[\{a/f^i \mid a \in Q_m, i < n\} \cup \{a/f^i \mid a \in Q_{m+1}, i \geq n\}]$ for $m \geq 0$, $n \geq 1$. (In interpreting this definition, we take $Q_0 := E$. In particular, $R_{01} = E[\{a/f^i \mid a \in Q\}]$.) Note that $R_{m1} = E[\{a/f^i \mid a \in Q_{m+1}\}]$. We claim that $E[1/f] \supset R_{01} \supset \cdots \supset R_{1,n+1} \supset R_{1n} \supset \cdots \supset R_{11} \supset \cdots \supset R_{2n} \supset \cdots \supset E$ is a maximal chain of rings between $E[1/f]$ and E. This claim is obviously sufficient to prove the lemma (and the negative answer to the infinite-dimensional case of the question raised in Remark 2.5 (b)).

To prove the claim, it suffices to verify the following four facts: $R_{01} \subset E[1/f]$ is a minimal ring extension; $R_{mn} \subset R_{m,n+1}$ is a minimal ring extension for each m, n; $\cup_n R_{mn} = R_{m-1,1}$; and $\cap_{m,n} R_{mn} = E$. To see the first of these facts, note that any proper ring extension T of R_{01} must necessarily contain an element of the form $(q+d)/f^i \notin R_{01}$, where $q \in Q$ and $d \in K[x]$. As $q/f^i \in R_{01}$, it follows that $d/f^i \in T \setminus R_{01}$. By unique factorization, we can reduce to $d \in K$, whence $1/f \in T$, as desired. To see the next fact, first note that if $T = R_{mn}$, it is easy to see that the ideals J_i defined above are given by $J_i = Q_m + f^i E$ if $i < n$ and by $J_i = Q_{m+1} + f^i E$ if $i \geq n$. Thus, if $R_{mn} \subset T \subseteq R_{m,n+1}$, we see that as the corresponding J_i's are almost all equal, the ideal J_n corresponding to T must satisfy $Q_{m+1} + f^n E \subset J_n \subseteq Q_m + f^n E$. However, the module $(Q_m + f^n E)/(Q_{m+1} + f^n E)$ has length 1, and so $T = R_{m,n+1}$, thus proving the second fact. The third fact follows easily from the definitions. Finally, for the fourth fact, $\cap_{m,n} R_{mn} = \cap_{m=1}^{\infty} R_{m1} = \cap_{m=1}^{\infty} E[\{a/f^i \mid a \in Q_{m+1}\}]$. As f is, without loss of generality, irreducible in E and $\cap_m Q_m = (0)$, it follows from unique factorization that this intersection is just E, which completes the proof. □

Acknowledgments. The authors wish to thank the referee for an extensive report which suggested some alternate, shorter proofs of some of our results and which encouraged us to reformulate our work independently of GCH as much as possible.

REFERENCES

1. J. Barwise, *Handbook of mathematical logic* (*Studies in logic and the foundations of mathematics*), Elsevier, Amsterdam, 1977.

2. E. Bastida and R. Gilmer, *Overrings and divisorial ideals of rings of the form $D + M$*, Michigan Math. J. **20** (1973), 79–95.

3. D.E. Dobbs, *On chains of overrings of an integral domain*, Int. J. Comm. Rings **1** (2002), 173–179.

4. ______, *On infinite chains of intermediate fields*, Inter. Elect. J. Alg. **11** (2012), 165–176.

5. D.E. Dobbs and B. Mullins, *On the lengths of maximal chains of intermediate fields in a field extension*, Comm. Alg. **29** (2001), 4487–4507.

6. R. Gilmer and W. Heinzer, *Jónsson ω_0-generated algebraic field extensions*, Pacific J. Math. **128** (1987), 81–116.

7. P.R. Halmos, *Naive set theory*, Van Nostrand, Princeton, 1960.

8. T.W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

9. N. Jacobson, *Lectures in abstract algebra*, Volume III, *Theory of fields and Galois theory*, Van Nostrand, Princeton, 1964.

10. M.M. Zuckerman, *Sets and transfinite numbers*, Macmillan, New York, 1974.

Department of Mathematics, University of Tennessee, Knoxville, TN 37996
Email address: **dobbs@math.utk.edu**

Department of Mathematics, The University of Texas at Austin, Austin, TX 78712
Email address: **heitmann@math.utexas.edu**