JOURNAL OF ALGEBRA **201,** 429–455 (1998)
ARTICLE NO. JA977307

Real Fields and Repeated Radical Extensions

I. M. Isaacs*

and

Mathematics Department, University of Wisconsin, 480 Lincoln Drive, Madison, Wisconsin 53706

Communicated by Walter Feit

Received February 21, 1997

1. INTRODUCTION

Recall that a field extension $F \subseteq L$ is said to be a *radical extension* if it possible to write $L = F[\alpha]$, where $\alpha \in L$ is an element with $\alpha^n \in F$ for some positive integer n. More generally, an extension $F \subseteq L$ is a *repeated radical extension* if there exist intermediate fields L_i with $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = L$ and such that each field L_i is a radical extension of L_{i-1} for $0 < i \le r$.

Given a polynomial $f(X)$ over a field F of characteristic 0, let S be a splitting field over F for f. Then as usual, we say that f is *solvable by radicals* if S is contained in some repeated radical extension of F. A celebrated theorem of Galois asserts that this occurs if and only if the associated Galois group $\mathrm{Gal}(S/F)$ is a solvable group.

It is well known that intermediate fields of repeated radical extensions need not themselves be repeated radical extensions of the ground field. The solvability of $\mathrm{Gal}(S/F)$, therefore, does not guarantee that S is a repeated radical extension of F, and so the phrase "contained in" in the statement of Galois' theorem is essential. For example, take $F = \mathbb{Q}$, the rational numbers, and consider the polynomial $f(X) = X^3 - 6X + 2$. It is easy to see that f has three real roots, and so we can take $S \subseteq \mathbb{R}$. Of

* E-mail: isaacs@math.wisc.edu.
† E-mail: moulton@math.wisc.edu.

0021-8693/98 $25.00

course, the cubic polynomial f is solvable by radicals; we can see this explicitly by calculating that the three roots of f are given by the formula $r = \alpha + 2/\alpha$, where α runs over the three complex cube roots of the complex number $-1 + \sqrt{-7}$. If S were a repeated radical extension of $\mathbb{Q}$, there would have to be some alternative way to express these roots in terms of *real* radicals. This is impossible, however, since f is easily seen to be irreducible, and it is a classical result that if an irreducible cubic polynomial has three real roots, then these roots definitely are not expressible in terms of real radicals. More generally, we have the following (known) result. (See [1] or Theorem 22.1 of [2]. Also, we include a somewhat simplified proof here, in Section 4.)

THEOREM A. *Let Q be any subfield of the real numbers $\mathbb{R}$ and suppose that $f \in Q[X]$ is irreducible and splits over $\mathbb{R}$. If any one of the roots of f lies in a real repeated radical extension of $\mathbb{Q}$, then* $\deg(f)$ *must be a power of* 2.

We show that at least in certain cases, intermediate fields of repeated radical extensions actually are repeated radical extensions. As in Theorem A, the ground field need not be the rational numbers; any field $Q \subseteq \mathbb{R}$ will suffice.

THEOREM B. *Suppose that Q is a real field and that $Q \subseteq L$ is a repeated radical extension with $|L:Q|$ odd. If $Q \subseteq K \subseteq L$, then K is a repeated radical extension of Q.*

We will show by example that the condition in Theorem B that the ground field Q should be real cannot be dropped. Our proof of Theorem B begins by observing that it is no loss to assume that $L \subseteq \mathbb{R}$, and to handle that case, we derive a useful characterization of real repeated radical extensions. In fact, this somewhat technical characterization, which appears as Theorem 3.1, can be viewed as one of the principal results of this paper. Theorem 3.1 also has other applications, and in particular, it can be used to prove the following result, which in some sense complements Theorem A.

THEOREM C. *Suppose that Q is a real field and that $f \in Q[X]$ is irreducible of odd degree. If f has some root α in a real repeated radical extension of Q, then α is the only real root of f.*

In Theorem B, we considered intermediate fields of odd-degree repeated radical extensions over a real field. It is perhaps somewhat surprising that we get a similar result in exactly the opposite case, where the degree of the extension is a power of 2. In that case, we do not even require that the ground field should be real; it is enough that its characteristic is different from 2. As we shall see, the proof of this result is much easier than that of Theorem B and, of course, its proof does not use the characterization of real repeated radical extensions in Theorem 3.1.

THEOREM D. *Suppose that $Q \subseteq L$ is a repeated radical extension of fields of characteristic different from* 2. *If $|L:Q|$ is a power of* 2 *and $Q \subseteq K \subseteq L$, then K is a repeated radical extension of Q.*

In fact, in the situation of Theorem D, we show that K is actually a repeated *quadratic* extension of Q. This suffices because when the characteristic is different from 2, the quadratic formula guarantees that every quadratic extension is obtained by adjoining a square root. Quadratic extensions are therefore automatically radical extensions in this case.

The full strength of the hypothesis that the fields are real is not actually needed for Theorem A. For that result, it suffices that the relevant field L should be *quasireal*, which we define to mean that L has characteristic 0 and that the only roots of unity it contains are ± 1. In fact, our characterization of real repeated radical extensions in Theorem 3.1 actually works for quasireal fields, and we prove it in that generality. In proving Theorems B and C, however, we use the realness assumptions more fully. But even those results can be generalized somewhat, and the real field $\mathbb{R}$ can be replaced with an arbitrary (but fixed) formally real field. (Recall that a field is *formally real* if -1 is not a sum of squares or, equivalently, if the field can be ordered.)

As we remarked, our proof of Theorem B does not go through if we work more generally with quasireal fields in place of real fields. In the case where the extension degree is a prime power, however, quasirealness does suffice. (And if the degree is a power of 2, then by Theorem D, we know that even this hypothesis is much too strong.) Our proof of this result depends on the characterization of quasireal repeated radical extensions in Theorem 3.1.

THEOREM E. *Let $Q \subseteq L$ be a repeated radical extension, where L is quasireal. If $|L:Q|$ is a prime power and $Q \subseteq K \subseteq L$, then K is a repeated radical extension of Q.*

2. PRIME-DEGREE EXTENSIONS

We begin with an easy, but useful, lemma and some simple consequences. Most of this material is well known.

(2.1) LEMMA. *Let $Q \subseteq L$ be fields and suppose that $L = Q[\alpha]$, where α^n lies in Q for some integer $n \geq 1$. Write $d = |L:Q|$. The following statements then hold.*

(a) *In any extension field of L, all roots of the minimal polynomial $\min_Q(\alpha)$ have the form $\delta\alpha$, where δ is a nth root of unity.*

(b) *We have $d \leq n$, and if $\alpha^d \in Q$, then d divides n.*

(c) *For some nth root of unity $\epsilon \in L$, we have $\epsilon\alpha^d \in Q$. In particular, if Q contains all nth roots of unity in L, then $\alpha^d \in Q$.*

Proof. Write $a = \alpha^n$, so that α is a root of $X^n - a \in Q[X]$. The minimal polynomial $f = \min_Q(\alpha)$ must therefore divide $X^n - a$, and hence each root β of f is also a root of $X^n - a$. Thus $\beta^n = a$, and it follows that $\beta = \delta\alpha$, as claimed.

Since $d = \deg(f)$, it follows that α^r cannot lie in Q for any positive exponent $r < d$, and in particular we have $d \leq n$. Writing $n = qd + r$ with $0 \leq r < d$, we see that $\alpha^r = \alpha^n(\alpha^d)^{-q}$, and this lies in Q if $\alpha^d \in Q$. It follows that r cannot be positive in this case, and thus d divides n.

Also, as $\deg(f) = d$, it follows from (a) that the product of the d roots of f in a splitting field (counting multiplicities) has the form $\epsilon\alpha^d$ for some nth root of unity ϵ in the splitting field. But this product equals $\pm f(0)$, and so it lies in Q, and hence in L. Since $\alpha^d \in L$, we deduce that $\epsilon \in L$, as required. ∎

The following pleasant application of Lemma 2.1 will be used in the proof of Theorem D.

(2.2) COROLLARY. *Let $f(X) = X^p - a \in Q[X]$, where Q is any field and p is a prime number. Then either f is irreducible or else it has a root in Q.*

Proof. Let α be a root of f in some extension field $E = Q[\alpha]$, and write $m = |E:Q|$. If $m = p$, then f is irreducible, and so we assume that $m < p$. In particular, m and p are coprime, and we can thus choose integers k and l such that $mk + pl = 1$.

Since $\alpha^p \in Q$, we know by Lemma 2.1(c) that $\epsilon\alpha^m \in Q$ for some pth root of unity ϵ. Thus

$$\epsilon^k\alpha = \epsilon^k\alpha^{mk}\alpha^{pl} = (\epsilon\alpha^m)^k(\alpha^p)^l \in Q.$$

Since $\epsilon^k\alpha$ is a root of f, this completes the proof. ∎

(2.3) LEMMA. *Let $Q \subseteq L$ be a radical extension and assume that $|L:Q| = p$, where p is an odd prime.*

(a) *If L is Galois over Q, then L contains some root of unity different from ± 1, and so L is not quasireal.*

(b) *If L is not Galois over Q, then $L = Q[\alpha]$ for some element α with $\alpha^p \in Q$.*

Proof. Write $L = Q[\alpha]$, where some power of α lies in Q, and consider the minimal polynomial $f = \min_Q(\alpha)$. If L is Galois over Q, then f has at least $\deg(f) = p \geq 3$ distinct roots in L. By Lemma 2.1(a), each of these roots has the form $\delta\alpha$ for some root of unity $\delta \in L$, and thus L contains three different roots of unity, at least one of which must be different from ± 1. This proves (a).

By Lemma 2.1(c), we know that $\epsilon\alpha^p \in Q$ for some root of unity $\epsilon \in L$, and we have $Q \subseteq Q[\epsilon] \subseteq L$. If L is not Galois over Q, however, then $L \neq Q[\epsilon]$. Since $|L:Q|$ is prime, we conclude that $Q[\epsilon] = Q$ and $\epsilon \in Q$, and it follows that $\alpha^p \in Q$, as required. ∎

As is suggested by these lemmas, we shall need to control the roots of unity in a field extension $Q \subseteq E$. For this purpose, it will be useful to consider intermediate fields F that are abelian extensions of Q and contain all roots of unity in E. (Recall that a field extension $Q \subseteq F$ is said to be *abelian* if it is a Galois extension such that $\mathrm{Gal}(F/Q)$ is an abelian group. Also, we include in the definition of "Galois" the assumption that the extension has finite degree.) Given any finite degree extension $Q \subseteq E$, it is clearly always possible to find such a field F: simply take F to be the field generated by Q and all roots of unity in E. It is useful to have a little more freedom in selecting F, however, and this is the purpose of the following result.

(2.4) LEMMA. *Let $Q \subseteq K \subseteq E$, where K is abelian over Q. Then there exists a field F with $K \subseteq F \subseteq E$ such that F is abelian over Q and contains all roots of unity in E.*

Proof. Let L be the field generated over Q by all roots of unity in E. Then L is Galois over Q, and hence the compositum $F = KL$ of K and L in E is also Galois over Q. Furthermore, since each of L and K is abelian over Q, it is easy to see that F is also abelian over Q, and this completes the proof. ∎

Given a characteristic 0 field extension $Q \subseteq L$, we want to be able to determine whether or not it is a repeated radical extension. We begin by choosing an arbitrary Galois extension E of Q that contains L and a field $F \subseteq E$ that is abelian over Q and contains all roots of unity in E. Our criterion (given in the next section) for L to be a repeated radical extension of Q will be expressed in terms of the fields E and F and certain associated Galois groups. It will be convenient to standardize our notation in this situation, and so we will generally write $G = \mathrm{Gal}(E/Q)$,

$U = \mathrm{Gal}(E/L)$, and $N = \mathrm{Gal}(E/F)$. Then $U \subseteq G$ and $N \lhd G$ and we define $M = U \cap N$, so that $M \lhd U$. We observe that $|G:U| = |L:Q|$ and that $|G:UN| = |L \cap F:Q|$. Furthermore, $G/N \cong \mathrm{Gal}(F/Q)$ is abelian.

We shall also need to consider finite subgroups of the multiplicative group $E^\times$ of the field E. Note that such subgroups are uniquely determined by their order. If $D \subseteq E^\times$ is a subgroup of order n, for example, then D is exactly the subgroup $\langle \delta \rangle$, where δ is a primitive nth root of unity in E. Since $G = \mathrm{Gal}(E/Q)$ acts on the cyclic group D and $U \subseteq G$, we can view D as a U-group: a group acted on by U.

For the remainder of this section, we focus on the case where L has prime degree p over Q. In this situation, of course, L cannot be a *repeated* radical extension of Q unless it is actually a radical extension. Also, since every quadratic extension of fields of characteristic different from 2 is radical, we need only consider primes $p > 2$. The following is our principal result in this situation.

(2.5) THEOREM. *Let $Q \subseteq L$ with $|L:Q| = p$, where p is an odd prime not equal to the characteristic of Q. Let $E \supseteq L$ be Galois over Q and suppose that $F \subseteq E$ is abelian over Q and contains the roots of unity in E. Let G and its subgroups, N, U, and M be as described above. Then L is a radical extension of Q not contained in F if and only if the following conditions hold.*

(i) $|N:M| = p$.

(ii) $M \lhd N$.

(iii) *N/M is U-isomorphic to a subgroup of $E^\times$.*

Given $Q \subseteq L$ as in Theorem 2.5, where $|Q:L|$ is prime and not equal to the characteristic, we see that L is separable over Q, and thus it really is possible to choose E as in the statement of the theorem. Once E is selected, we have seen that it is easy to find an appropriate field F.

We will apply Theorem 2.5 only in the case where the field L is quasireal. As we shall see, L cannot be contained in F in that situation, and this yields a slight simplification of the result. Before proceeding with the proof of Theorem 2.5, we present the quasireal version as a corollary. (Recall from Section 1 that a quasireal field is a field of characteristic 0 in which the only roots of unity are ± 1.)

(2.6) COROLLARY. *In the situation of Theorem* 2.5, *assume that L is quasireal. Then L is radical over Q if and only if conditions* (i), (ii), *and* (iii) *hold*.

Proof. By Theorem 2.5, all that must be proved is that if L is radical over Q and is contained in F, then L cannot be quasireal. But F is abelian over Q, and so L is Galois over Q and thus by Lemma 2.3(a), it is not quasireal. ∎

Our proof of Theorem 2.5 relies on well-known facts from the theory of representations of Frobenius groups. Since some of this material may be unfamiliar to some readers of this paper, we present a simple lemma that is sufficient for our purposes. Recall that a set $\mathscr{P}$ of subgroups of a group G is a *partition* of G if $\bigcup \mathscr{P} = G$ and $H \cap K = 1$ for distinct members $H, K \in \mathscr{P}$.

(2.7) LEMMA. *Let $\mathscr{P}$ be a partition of a finite group G, and suppose that G acts via automorphisms on an abelian group A. If A contains an element with order not dividing $|\mathscr{P}| - 1$, then $\mathbf{C}_A(H) > 1$ for some member $H \in \mathscr{P}$.*

Proof. Write A additively and fix an element $a \in A$ with order not dividing $|\mathscr{P}| - 1$. For each subgroup $X \subseteq G$, define $a_X = \sum_{x \in X} a^x$ and note that $a_X \in \mathbf{C}_A(X)$. We can assume, therefore, that $a_H = 0$ for all members $H \in \mathscr{P}$, and also that $a_G = 0$. Since $\mathscr{P}$ is a partition of G, however, this yields

$$0 = \sum_{H \in \mathscr{P}} a_H = (|\mathscr{P}| - 1)a + a_G = (|\mathscr{P}| - 1)a.$$

This contradicts our choice of a and completes the proof. ∎

The specific application of Lemma 2.7 that we shall need concerns a Frobenius group F with kernel N and complement H. If F acts on a nontrivial vector space in characteristic not dividing $|N|$, then either N or H must have nontrivial fixed points. This follows since F is partitioned by N and the $|N|$ conjugates of H. If N has no nontrivial fixed points, then by the lemma, some conjugate of H has nontrivial fixed points, and it is immediate that H also must have nontrivial fixed points.

Before we begin the proof of Theorem 2.5, we mention one other basic result from group representation theory: if an elementary abelian p-group P of order p^2 acts on a nonzero vector space, then some subgroup of order p in P has nontrivial fixed points on the space. This is immediate from the fact that an abelian group having a faithful irreducible representation must be cyclic, but it is amusing that Lemma 2.7 can also be used to prove this, at least in the important case where the characteristic is different from p. Since P is partitioned into $p + 1$ subgroups of order p, we see by the lemma that one of those subgroups must have nontrivial fixed points.

Proof of Theorem 2.5. Suppose first that $L \not\subseteq F$ and that L is a radical extension of Q. Since $|L:Q|$ is prime, we have $L \cap F = Q$, and hence $UN = G$. It follows that $|N:M| = |G:U| = |L:Q| = p$, proving (i). Furthermore, all roots of unity in L are in F, and hence they lie in Q. Since $|L:Q| = p$ and we are assuming that L is radical over Q, we can apply Lemma 2.1(c) and write $L = Q[\alpha]$, where $\alpha^p \in Q$.

Choose $\tau \in N - M$ and note that since $\tau \notin U$, we have $\alpha^{\tau} \neq \alpha$. But τ fixes $\alpha^p \in Q$, and it follows that $\alpha^{\tau} = \epsilon\alpha$ for some primitive pth root of unity $\epsilon \in E$. Write $D = \langle \epsilon \rangle \subseteq E^{\times}$, and note that $|D| = p$.

Since $L[\epsilon]$ is a splitting field over Q for the polynomial $X^p - \alpha^p \in Q[X]$, we see that $L[\epsilon]$ is Galois over Q, and hence the compositum $L[\epsilon]F$ is also Galois over Q. However, $\epsilon \in F$, and thus $L[\epsilon]F = LF$, and this corresponds to the subgroup $U \cap N = M$. It follows that $M \lhd G$, and in particular, $M \lhd N$ and (ii) is proved.

Since $|N/M| = p = |D|$, we see that to prove (iii), it suffices to check that the actions of an arbitrary element $\sigma \in U$ on D and on N/M agree. Recall that we have $\tau \in N - M$ with $\alpha^{\tau} = \epsilon\alpha$. The coset $M\tau$ generates N/M, and thus $\tau^{\sigma} \equiv \tau^{s} \mod M$ for some integer s. Also, s determines the action of σ on N/M, and since ϵ generates D, it suffices to show that $\epsilon^{\sigma} = \epsilon^{s}$. Now ϵ is fixed by τ (because $\epsilon \in F$ and $\tau \in N = \mathrm{Gal}(E/F)$) and α is fixed by U, which contains both M and σ. We can now compute that

$$\alpha\epsilon^{\sigma} = (\alpha\epsilon)^{\sigma} = \alpha^{\tau\sigma} = \alpha^{\sigma^{-1}\tau\sigma} = \alpha^{\tau^{\sigma}} = \alpha^{\tau^{s}} = \alpha\epsilon^{s}.$$

Thus $\epsilon^{\sigma} = \epsilon^{s}$, as desired, and hence D and N/M are U-isomorphic and (iii) holds.

Conversely now, assume the three conditions. By (i), we have $|UN:U| = |N:M| = p = |L:Q| = |G:U|$, and thus $UN = G$. It follows that $L \cap F = Q$ and, in particular, $L \nsubseteq F$. It remains to show that L is radical over Q.

Conditions (ii) and (iii) tell us that $E^{\times}$ has a subgroup D that is U-isomorphic to N/M, which we know has order p. In particular, $D = \langle \epsilon \rangle$, where ϵ is a primitive pth root of unity in E. Write $K = L[\epsilon]$ and $C = \mathrm{Gal}(E/K)$. Thus C is exactly the set of elements in $U = \mathrm{Gal}(E/L)$ that fix ϵ, and hence C is the kernel of the action of U on D, and in particular, $C \lhd U$. Also, $\epsilon \in F$, and thus M fixes ϵ, and we have $M \subseteq C$. By the U-isomorphism between D and N/M, we see that C acts trivially on N/M. Thus $[C, N] \subseteq M \subseteq C$, and therefore N normalizes C. But $UN = G$ and U normalizes C, and we deduce that $C \lhd G$, and hence K is Galois over Q.

Now G induces Q-linear transformations on K, and we write $\overline{G}$ to denote the image of G in the full general linear group $\Gamma = GL_Q(K)$. The map $\sigma \mapsto \overline{\sigma}$ is a homomorphism from G onto $\overline{G}$, and its kernel is $\mathrm{Gal}(E/K) = C$. Since $C \cap N = M$, we see that $\overline{N}$ has order p and also that $\overline{U}$ acts faithfully on $\overline{N}$ by conjugation. In particular, $\overline{G} = \overline{UN}$ is a Frobenius group with complement $\overline{U}$ and kernel $\overline{N}$. (Technically, the definition of a "Frobenius group" requires that the complement should be nontrivial, which may not be the case in our situation.)

Since $D \subseteq K$, there is another subgroup of order p in Γ that is of interest to us, a subgroup different from $\overline{N}$. This is the group Δ consisting of scalar multiplications on K by elements of D. (Note that $\overline{N}$ fixes the element $1 \in K$ while Δ does not, and thus $\overline{N}$ and Δ really are different.) If $\mu \in \Delta$ is scalar multiplication by $\delta \in D$ and a is any element of K, then for $\sigma \in G$, we have

$$(a)\mu^{\sigma} = (a)\sigma^{-1}\mu\sigma = \left(a^{\sigma^{-1}}\delta\right)^{\sigma} = a\delta^{\sigma}.$$

It follows that $\overline{G}$ normalizes Δ in Γ and this calculation also shows that Δ and D are isomorphic as G-groups. Since D and $\overline{N}$ are U-isomorphic by hypothesis, we conclude that Δ and $\overline{N}$ are $\overline{U}$-isomorphic.

Recall that $\overline{N}$ normalizes and is distinct from Δ. It follows that $\overline{N}\Delta$ is an elementary abelian subgroup of Γ having order p^2, and we write $A = \overline{N}\Delta$. Since $\overline{U}$ acts in the same way on each of Δ and $\overline{N}$, we deduce that every subgroup of A is $\overline{U}$-invariant and hence is normal in $\overline{U}A = \overline{G}\Delta$.

Since we are assuming that Q does not have characteristic p, Maschke's theorem applies and we see that K is completely reducible as a QN-module. We can thus write the Q-space K as the direct sum of the subspace consisting of the N-fixed points and a unique complementary N-invariant Q-subspace V, on which N acts without fixed points. Furthermore, since N acts nontrivially on K, we see that V is nonzero. (Of course, the Q-subspace $V \subseteq K$ is not a sub*field* of K because $1 \notin V$.) Since $\overline{N} \lhd \overline{U}A$, the uniqueness of V guarantees that V is invariant under $\overline{U}A$.

As A is noncyclic of order p^2 and acts on $V > 0$, there must be some subgroup $B \subseteq A$ of order p such that B has nontrivial fixed points on V. (This is one of our applications of Lemma 2.7.) Let $W \subseteq V$ be the (nonzero) fixed-point space of B. We know that $B \lhd \overline{U}A$, and it follows that W is invariant under $\overline{U}A$. (This is the key point where we use the assumption that the actions of U on N/M and D agree. It is the assumption that underlies the fact that every subgroup of A is normalized by $\overline{U}$.)

The Frobenius group $\overline{U}\overline{N}$ acts on W, and $\overline{N}$ has no nonzero fixed points in W because $W \subseteq V$ and $\overline{N}$ has no nonzero fixed points in V. It follows via Lemma 2.7 that there exists a nonzero element $\alpha \in W$ fixed by $\overline{U}$, and thus α is fixed by U, and $\alpha \in L$. Also, since $\alpha \in V$, we know that α is not fixed by $\overline{N}$, and thus $\alpha \notin Q$. Therefore $L = Q[\alpha]$, and it suffices to show that $\alpha^p \in Q$ in order to prove that L is a radical extension of Q.

Recall that $\alpha \in W$ is fixed by the subgroup $B \subseteq A = \overline{N}\Delta$. But $B \neq \Delta$ since Δ has no nonzero fixed points on K, and it follows that B contains some element of the form $b = \bar{\tau}\mu$, where $\bar{\tau}$ generates $\overline{N}$ and $\mu \in \Delta$ is multiplication by some pth root of unity δ. We have

$$\alpha = (\alpha)b = (\alpha)\bar{\tau}\mu = (\alpha^{\tau})\delta,$$

and thus $\alpha^{\tau} = \alpha\delta^{-1}$. We deduce that τ fixes α^{p}, which is therefore fixed by all of $\overline{N}$. Since U fixes α, it also fixes α^{p}, and we conclude that α^{p} is fixed by $\overline{UN} = \overline{G}$. Thus α^{p} is fixed by G, and the proof is complete. ∎

3. CHARACTERIZING QUASIREAL REPEATED RADICAL EXTENSIONS

The following is our principal result in this section.

(3.1) THEOREM. *Suppose $Q \subseteq L$, where L is quasireal. Let $E \supseteq L$ be Galois over Q and suppose that $F \subseteq E$ is abelian over Q and contains all roots of unity in E. As usual write $G = \mathrm{Gal}(E/Q)$ and let $N = \mathrm{Gal}(E/F)$, $U = \mathrm{Gal}(E/L)$, and $M = N \cap U$. Then L is a repeated radical extension of Q if and only if there is a chain of U-invariant subgroups M_i, where $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = N$, and all of the following conditions hold.*

(i) *$|F \cap L{:}Q|$ is a power of 2.*

(ii) *Each index $|M_i{:}M_{i-1}|$ is prime.*

(iii) *$M_{i-1} \lhd M_i$ for each integer i with $0 < i \leq r$.*

(iv) *Each factor M_i/M_{i-1} is U-isomorphic to a subgroup of $E^{\times}$.*

In order to understand these conditions better, it seems worthwhile to play with them a little before we proceed with the proof. Assuming (ii), (iii), and (iv), let $D_i \subseteq E^{\times}$ be U-isomorphic to M_i/M_{i-1}. We see that $|D_i| = |M_i/M_{i-1}|$ is prime, and so the subgroups D_i are exactly the groups $\langle \delta \rangle$ as δ runs over primitive pth roots of unity in E for prime divisors p of $|N{:}M|$. In particular, (iv) guarantees the existence in E of all of these pth roots of unity. To see exactly which primes these are, observe that $|N{:}M| = |NU{:}U| = |L{:}L \cap F|$. If (i) holds, then the odd prime divisors of $|N{:}M|$ are exactly the odd prime divisors of $|L{:}Q|$, and this shows that a consequence of the four conditions is that E contains a primitive pth root of unity for each prime divisor p of $|L{:}Q|$.

Next, observe that $G/N \cong \mathrm{Gal}(F/Q)$, which is abelian, by assumption. Assuming (ii) and (iii), we see that the factor groups M_i/M_{i-1} are abelian, and thus successive terms of the derived series of G are contained in the subgroups M_i with decreasing subscripts i. In particular, this tells us that the terms of the derived series of G eventually lie within M, and hence G/H is solvable for every normal subgroup H of G with $H \supseteq M$. In particular, this holds for all normal subgroups of G that contain U. Translating this last conclusion into field theory, we see that (ii) and (iii) guarantee that if $Q \subseteq K \subseteq L$ and K is Galois over Q, then $\mathrm{Gal}(K/Q)$ is solvable. Of course, this is exactly what we would expect by Galois' theorem if L really is a repeated radical extension of Q.

We begin working toward a proof of Theorem 3.1 with the following easy lemma. (A weaker form of this result is Theorem 22.14 of [2], which appears there with an unnecessarily complicated proof.)

(3.2) LEMMA. *Suppose that L and S are, respectively, a radical extension and a Galois extension of some field Q. If both L and S are quasireal, then* $|L \cap S{:}Q| \leq 2$.

Proof. Write $L = Q[\alpha]$, where some power of α is in Q, and let $m = |L{:}L \cap S|$. Since L is quasireal, the only roots of unity it contains are ± 1, and these, of course, lie in $L \cap S$. It follows by Lemma 2.1(c) that $\alpha^m \in L \cap S$ and we set $\beta = \alpha^m$ and $F = Q[\beta] \subseteq L \cap S$. Observe that α is a root of the polynomial $f(X) = X^m - \beta \in F[X]$, and thus we have

$$\begin{aligned}\deg(f) &= m = |L{:}L \cap S| = |F[\alpha]{:}L \cap S| \leq |F[\alpha]{:}F| \\ &= \deg(\min_F(\alpha)) \leq \deg(f).\end{aligned}$$

Equality must hold throughout, and we deduce that $L \cap S = F = Q[\beta]$.

Write $g = \min_Q(\beta)$ and note that g splits over S since by hypothesis, S is Galois over Q. But some power of α lies in Q, and thus the same is true for β, and it follows by Lemma 2.1(a) that every root of g in S has the form $\epsilon\beta$ for some root of unity $\epsilon \in S$. As S is quasireal, the only possibilities are $\epsilon = \pm 1$, and thus g has at most two roots. The roots of g are distinct, however, and it follows that $|L \cap S{:}Q| = \deg(g) \leq 2$. ∎

The following result is closely related to Theorems 22.12 and 22.15 of [2].

(3.3) THEOREM. *Let $Q \subseteq E$, where E is quasireal. Suppose that L and S are subfields of E that are, respectively, a repeated radical extension and a Galois extension of Q. Then $L \cap S$ is a repeated quadratic extension of Q.*

Proof. We can assume that $L > Q$, and so we can choose a radical extension F of Q such that $Q < F \subseteq L$. Since S is Galois over Q, it follows by Lemma 3.2 that $|F \cap S{:}Q| \leq 2$.

Now L is a repeated radical extension of F and the compositum FS is Galois over F. As $|L{:}F| < |L{:}Q|$, we can work by induction on $|L{:}Q|$ and apply the inductive hypothesis with F in place of Q and FS in place of S. We deduce that D is a repeated quadratic extension of F, where we have written $D = L \cap FS$. In other words, there exists a tower of degree 2 field extensions $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = D$.

Since S is Galois over Q, we can apply the so-called theorem on natural irrationalities (see Theorem 18.22 of [2]) to see that $|FS:F| = |S:F \cap S|$. More generally, if X is any field such that $F \subseteq X \subseteq FS$, we have $|FS:X| = |S:X \cap S|$, and we deduce that $|X:F| = |X \cap S:F \cap S|$. If $X \subseteq Y$ are two consecutive fields in the tower $\{F_i\}$ of degree 2 extensions running from F to D, it follows that $|Y \cap S:X \cap S| = |Y:X| = 2$. We conclude that the fields $F_i \cap S$ form a tower of degree 2 extensions running from $F_0 \cap S = F \cap S$ up to $F_m \cap S = D \cap S = L \cap S$. Since $|F \cap S:Q|$ is at most 2, it follows that $L \cap S$ is a repeated quadratic extension of Q, as required. ∎

We mention that in the situation of Theorem 3.3, where we are dealing with fields of characteristic zero, quadratic extensions are automatically radical extensions, and thus in the notation of the theorem, $L \cap S$ is a repeated radical extension of Q.

(3.4) COROLLARY. *Let $Q \subseteq S \subseteq L$, where L is quasireal and S is Galois over Q. If L is a repeated radical extension of Q, then $|S:Q|$ is a power of 2. Conversely, if $|S:Q|$ is a power of 2, then at least S is a repeated radical extension of Q.*

Proof. If L is a repeated radical extension of Q, then we can take $E = L$ in Theorem 3.3, and we deduce that S is a repeated quadratic extension of Q, and hence $|S:Q|$ is a power of 2. Conversely, if $|S:Q|$ is a power of 2, then $\mathrm{Gal}(S/Q)$ is a 2-group, and by elementary group theory and Galois theory, we see that S is a repeated quadratic extension and hence it is a repeated radical extension of Q. ∎

We need one further preliminary result.

(3.5) LEMMA. *Let $Q \subseteq L$, where L is quasireal. Then L is a repeated radical extension of Q if and only if there is a tower of fields $Q = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$ such that the extensions $L_{i-1} \subseteq L_i$ are radical extensions of prime degree for each integer i with $0 < i \leq m$.*

Proof. Since the sufficiency of the condition is obvious, we assume that $L > Q$ is a repeated radical extension, and we proceed to construct the fields L_i. Working by induction on $|L:Q|$, we see that it suffices to construct $L_1 \subseteq L$ such that L_1 is a radical extension of prime degree over Q.

Since L is a proper repeated radical extension of Q, we can choose an element $\alpha \in L$ such that $\alpha \notin Q$ but $\alpha^n \in Q$ for some positive integer n. Choose α so that n is as small as possible and observe that this forces n to be a prime number. Now write $L_1 = Q[\alpha]$, so that L_1 is radical over Q. Setting $d = |L_1:Q|$, we have $d \leq n$ by Lemma 2.1(b). Since L is quasireal, however, all roots of unity in L_1 lie in Q, and thus $\alpha^d \in Q$ by Lemma 2.1(c). By the minimality of n, we deduce that $d = n$, and d is prime, as required. ∎

We can now present the proof of Theorem 3.1, which is our characterization of quasireal repeated radical extensions. Essentially, the proof proceeds by repeated application of Theorem 2.5 and Corollary 2.6

Proof of Theorem 3.1. Suppose first the $F \cap L = Q$. In this situation, we show that L is a repeated radical extension of Q if and only if there is an appropriate chain of subgroups for which conditions (ii), (iii), and (iv) of the theorem hold. In view of Lemma 3.5, therefore, we want to show that the the three conditions are equivalent to the existence of a tower of fields from Q to L, where each successive extension is radical and of prime degree.

By Galois theory, we know that every intermediate field A with $Q \subseteq A \subseteq L$ corresponds to a subgroup W with $U \subseteq W \subseteq G$ such that $|L:A| = |W:U|$. Also, in our situation, where $UN = G$, there is a bijective correspondence between subgroups W with $U \subseteq W \subseteq G$ and U-invariant subgroups R with $M \subseteq R \subseteq N$. (Subgroups W and R correspond if $R = W \cap N$ or, equivalently, $W = UR$.) If W and R correspond in this situation, we have $|W:U| = |R:M|$. It follows from all of this that the existence of a chain satisfying condition (ii) is exactly equivalent to the existence of a tower of fields from Q to L, where each successive extension has prime degree.

Now consider intermediate fields A and B with $Q \subseteq A \subseteq B \subseteq L$, where $|B:A| = p$, a prime number, and let R and S, respectively, be the corresponding U-invariant subgroups of N, so that $M \subseteq S \subseteq R \subseteq N$ and $|R:S| = p$. Writing $W = \mathrm{Gal}(E/A)$ and $V = \mathrm{Gal}(E/B)$, we have $R = W \cap N$ and $S = V \cap N = V \cap R$. It suffices to show that B is a radical extension of A if and only if $S \lhd R$ and R/S is U-isomorphic to a subgroup of $E^{\times}$.

If $p = 2$, then B is a quadratic extension of A, and this is automatically a radical extension. Also in this case, $|R:S| = 2$, and so $S \lhd R$ and R/S is U-isomorphic to the subgroup $\langle -1 \rangle \subseteq E^{\times}$. We can thus assume that $p > 2$ and we appeal to Theorem 2.5 and Corollary 2.6 with A and B in place of the fields Q and L of those results.

Our present field E is Galois over A, and so it will serve as the field called E in Theorem 2.5. For the field F of Theorem 2.5, we take the compositum AF. (This is abelian over A by the theorem on natural irrationalities, and it certainly contains all roots of unity in E.) In Theorem 2.5, we had $U = \mathrm{Gal}(E/L)$, and the corresponding group in the present situation is $V = \mathrm{Gal}(E/B)$. Also in Theorem 2.5 we had $N = \mathrm{Gal}(E/F)$, and here, this corresponds to $\mathrm{Gal}(E/AF) = \mathrm{Gal}(E/A) \cap N = R$. Finally, the group M of Theorem 2.5 was $U \cap N$, and the corresponding group here is $V \cap R = S$. We can thus apply Corollary 2.6 with V, R, and S in place of U, N, and M, respectively, and it follows that B is radical over A if and only if $S \lhd R$ and R/S is V-isomorphic to a subgroup of $E^{\times}$. All that remains in this case, therefore, is to show that R/S is U-isomorphic to $\langle \epsilon \rangle$ if and only if it is V-isomorphic to $\langle \epsilon \rangle$, where ϵ is a primitive pth root of unity in E. Since $U \subseteq V$, we see that if R/S and $\langle \epsilon \rangle$ are V-isomorphic, they are automatically U-isomorphic. To prove the converse, we observe that S acts trivially on R/S and also that S acts trivially on $\langle \epsilon \rangle$ since $\epsilon \in F$ and $S \subseteq N = \mathrm{Gal}(E/F)$. but $V = US$, and so we see that if R/S and $\langle \epsilon \rangle$ are U-isomorphic, they must also be V-isomorphic, as required.

Finally, we consider the general case, where we do not assume that $L \cap F = Q$. Applying the previous argument with $L \cap F$ in place of Q (and UN in place of G) we see that L is a repeated radical extension of $L \cap F$ if and only if conditions (ii), (iii), and (iv) hold. Observe that $L \cap F$ is a Galois extension of Q because F is abelian over Q. If condition (i) holds, so that $|L \cap F{:}Q|$ is a power of 2, then $L \cap F$ is a repeated radical extension of Q by Corollary 3.4. If all four conditions hold, therefore, L is a repeated radical extension of $L \cap F$, which is a repeated radical extension of Q, and thus L is a repeated radical extension of Q, as required. Conversely, if L is a repeated radical extension of Q, then condition (i) holds by Corollary 3.4. Also L is a repeated radical extension of $L \cap F$ in this case, and thus (ii), (iii), and (iv) hold. This completes the proof. ∎

4. REPEATED QUADRATIC EXTENSIONS

Before we proceed to prove Theorems B and C, which are our main applications of Theorem 3.1, we offer an easy proof of the known Theorem A, and we prove Theorem D. Our proofs rely on some of the preliminary results in Sections 2 and 3, but they are independent of the characterization of quasireal repeated radical extensions in Theorem 3.1. We begin with an easy lemma about repeated quadratic extensions. (Recall that a quadratic extension is automatically a radical extension when the characteristic is different from 2.)

(4.1) LEMMA. *Let $Q \subseteq L$ be a repeated quadratic extension of fields of characteristic different from* 2, *and let E be the normal closure of L over Q. Then E is Galois over Q and $|E{:}Q|$ is a power of* 2. *In this situation, every intermediate field between Q and E is a repeated quadratic extension of Q.*

Proof. The degree $|L{:}Q|$ is a power of 2, and hence it is not divisible by the characteristic of Q. It follows that L is separable over Q, and hence E is actually Galois over Q. We write $G = \mathrm{Gal}(E/Q)$.

As L is a repeated quadratic extension of Q, so too is L^σ for every automorphism $\sigma \in G$. Since the compositum of two repeated quadratic extensions of Q is again a repeated quadratic extension, we see that the field $J = (\{L^\sigma | \sigma \in G\})$ is also a repeated quadratic extension of Q. But J

is invariant under G, and thus J is Galois over Q, and we deduce that $J = E$. Thus E is a repeated quadratic extension of Q and $|E:Q|$ is a power of 2, as desired.

Now G is a 2-group, and thus for every subgroup $H \subseteq G$, there is a chain of subgroups running from H to G, each of index 2 in the next subgroup. It follows by elementary Galois theory that if $Q \subseteq K \subseteq E$, then there is a chain of fields running from K to Q, each of degree 2 over the next field. This completes the proof. ∎

The following theorem includes Theorem A and generalizes it to quasireal fields.

(4.2) THEOREM. *Let $Q \subseteq E$, where E is quasireal, and suppose $f \in Q[X]$ is irreducible and splits over E. If some root of f lies in a repeated radical extension of Q contained in E, then the splitting field for f over Q in E is a repeated radical extension of* 2*-power degree over Q. Also,* $\deg(f)$ *is a power of* 2.

Proof. Let $L \subseteq E$ be a repeated radical extension of Q containing a root α of f. Then $\alpha \in L \cap S$, where S is the splitting field for f over Q in E, and it follows that S is the normal closure of $L \cap S$ over Q. By Theorem 3.3, we know that $L \cap S$ is a repeated quadratic extension of Q, and hence $\deg(f) = |Q[\alpha]:Q|$ is a power of 2. Also, by Lemma 4.1, we see that $|S:Q|$ is a power of 2 and that S is a repeated quadratic extension of Q, as required. ∎

Finally, we establish Theorem D by proving the following result.

(4.3) THEOREM. *Suppose that $Q \subseteq L$, where L is a repeated radical extension of fields of characteristic different from* 2. *If $|L:Q|$ is a power of* 2 *and $Q \subseteq K \subseteq L$, then K is a repeated quadratic extension of Q.*

Proof. (Lenstra). By Lemma 4.1, it suffices to show that L is a repeated quadratic extension of Q. Since $L \supseteq Q$ is a repeated radical extension and we can assume that $L > Q$, we can choose an element $\alpha \in L$ such that $\alpha \notin Q$, but $\alpha^p \in Q$ for some positive integer p. If we choose α such that p is as small as possible, it is clear that p is prime.

Now let $K = Q[\alpha]$. Then L is a repeated radical extension of 2-power degree over K, and so if we work by induction on $|L:Q|$, it follows by the inductive hypothesis that L is a repeated quadratic extension of K. It suffices, therefore, to show that K is a repeated quadratic extension of Q.

Let $a = \alpha^p \in Q$, so that α is a root of the polynomial $f(X) = X^p - a$. If f is irreducible over Q, then $|K:Q| = \deg(f) = p$. But $|K:F|$ is a power of 2 and p is prime, and so we see that $|K:F| = 2$, and K is quadratic over Q, as desired. If, on the other hand, f reduces over Q, then by Corollary 2.2, we deduce that f has some root $\beta \in Q$. Then α/β is a pth root of unity that generates K over Q. In this case, K is Galois over Q, and since we know that $|K:Q|$ is a power of 2, it follows that K is a repeated quadratic extension of Q. ∎

5. SOME GROUP THEORY

We shall need the following result for our proof of Theorem B.

(5.1) LEMMA. *Let $M \subseteq R \subseteq N$ with $M \lhd \lhd N$, where N is a finite group. Suppose that $\sigma \in \operatorname{Aut}(N)$ has order 2 and that M is σ-invariant. If σ acts fixed-point-freely on each factor in some σ-invariant subnormal series from M up to N, then $R \lhd \lhd N$.*

We mention that if a group H acts via automorphisms on a finite group N, and H stabilizes some subnormal subgroup M of N, then there necessarily exists an H-invariant subnormal series from M up to N. (This is a consequence of Lemma 5.3, below.) In Lemma 5.1, therefore, it is not necessary to assume the existence of the σ-invariant series from M to N; the key hypothesis is that the action of σ on each factor in some such series is fixed-point free. As we shall see in Lemma 5.4, if the action of σ on the factors of a σ-invariant subnormal series from M to N is fixed-point free, then the same will be true for every such series.

Observe that we did not assume that R is σ-invariant in the statement of Lemma 5.1, and in fact, in the situation of that lemma, we can deduce that R must be σ-invariant. (When we apply the lemma in the proof of Theorem B, however, it will be clear that R is σ-invariant.)

The hypothesis that σ has order 2 in Lemma 5.1 is unnecessarily restrictive. If we are willing to assume that R is σ-invariant, then the conclusion that $R \lhd \lhd N$ holds if the order of σ is any prime number. This result is deeper than Lemma 5.1, however, because it relies on J. Thompson's famous theorem that a group admitting a fixed-point free automorphism of prime order p must be nilpotent. As is well known, the conclusion of this theorem is a triviality when $p = 2$ and so the proof of Lemma 5.1 does not rely on Thompson's result. We have decided, however, to state and prove the more general theorem.

(5.2) THEOREM. *Let σ be an automorphism of prime order p of a finite group N. Suppose that $M \lhd \lhd N$ is σ-invariant and that σ acts fixed-point-freely on each factor in some σ-invariant subnormal series from M to N. Let $M \subseteq R \subseteq N$ and if $p > 2$, assume that R is σ-invariant. Then $R \lhd \lhd N$ and it is σ-invariant even when $p = 2$.*

The following well-known result is helpful, but it is not strictly necessary for the proof of Theorem 5.2. We shall really need this result later, however.

(5.3) LEMMA. *Let $M \lhd \lhd N$, where N is a finite group. Then there exist subgroups M_i such that $M = M_0 \lhd M_1 \lhd \cdots \lhd M_r = N$ and every automorphism of N that stabilizes M also stabilizes each of the subgroups M_i.*

Proof. There is nothing to prove if $M = N$, and so we can assume that $M \subseteq M^N < N$, where M^N denotes the normal closure of M in N. (Note that the normal closure M^N is proper in N because M is proper and subnormal.) Working by induction on $|N:M|$, we can find a subgroup chain $M = M_0 \lhd M_1 \lhd \cdots \lhd M_{r-1} = M^N$, where each subgroup M_i is stabilized by the automorphisms of M^N that stabilize M. Since the automorphisms of N that stabilize M also stabilize M^N, the result follows by defining $M_r = N$. ∎

(5.4) LEMMA. *Let $M \lhd \lhd N$ and suppose M is σ-invariant, where $\sigma \in$ $\mathrm{Aut}(N)$ has prime order p. If σ acts fixed-point-freely on all factors in some σ-invariant subnormal series from M up to N, then σ acts fixed-point-freely on every section R/S with $M \subseteq S \lhd R \subseteq N$, where R and S are σ-invariant.*

Proof. Let $\mathscr{X}$ be a σ-invariant subnormal series from M to N such that σ acts fixed-point-freely on each factor. We claim that the only σ-invariant right coset of M in N is M itself, and thus $|N:M| \equiv 1 \bmod p$. To see this, suppose that the coset My is σ-invariant and consider the minimal term Y Of $\mathscr{X}$ that contains y. If $Y = M$, then $My = M$ as desired, and so we suppose that $Y > M$ and derive a contradiction. Consider the term X just below Y in $\mathscr{X}$. Then $X \lhd Y$, both X and Y are σ-invariant, and by hypothesis, the action of σ on Y/X is fixed-point free. But $Xy = X(My)$ is σ-invariant, and thus $y \in X$, contradicting our choice of Y.

Now let R and S be as in the statement of the lemma and suppose that σ stabilizes the coset $Sr \in R/S$. As $M \subseteq S$, we see that Sr is a union of $|S:M|$ right cosets of M, and these are permuted by σ. But $|S:M|$ divides $|N:M|$, which is not divisible by p. It follows that σ fixes one of the cosets of M in Sr, and thus $M \subseteq Sr$. We conclude that $Sr = S$, as required. ∎

Under the hypotheses of Theorem 5.2, we see by Lemma 5.4 that if $M \subseteq D \lhd N$ for some σ-invariant subgroup D, then σ acts fixed-point-freely on N/D, which is therefore nilpotent by Thompson's theorem. Also, if $p = 2$, then σ inverts all elements of N/D, which is therefore abelian. In this case, every subgroup R satisfying $D \subseteq R \subseteq N$ is σ-invariant.

If $M \lhd N$ in Theorem 5.2, therefore, then N/M is nilpotent, and it is immediate that $R \lhd \lhd N$. The significance of Theorem 5.2 is that it is not necessary to assume that M is normal; subnormality is sufficient.

Proof of Theorem 5.2. The result is trivially true when $R = N$, and so we can assume that $R < N$, and we work by double induction: first on $|N|$ and then on $|N:R|$. If there exists a subgroup S with $R < S < N$, where S

is σ-invariant if $p > 2$, then by the inductive hypothesis applied to the situation $S \subseteq N$, we deduce that $S \lhd \lhd N$ and that S is σ-invariant (even if $p = 2$). By Lemma 5.3 (or by intersecting the given series with S), we see that there is a σ-invariant subnormal series from M to S. Also, by Lemma 5.4, the hypotheses apply with S in place of N (with the same subgroups M and R). It follows by the inductive hypothesis applied in the situation $R \subseteq S$ that R is σ-invariant and is subnormal in S, and we are done in this case. We can thus suppose that R is a maximal subgroup of N if $p = 2$, and that it is a maximal σ-invariant subgroup if $p > 2$.

Let $H = M^N$, the normal closure, and write $D = R \cap H$. Observe that $H < N$ because M is proper and subnormal in N, and $D \lhd R$ since $H \lhd N$. Also, H is σ-invariant because M is, and D is σ-invariant if $p > 2$. By Lemmas 5.3 and 5.4, therefore, we can apply the inductive hypothesis to the situation $M \subseteq D \subseteq H$, and we deduce that $D \lhd \lhd H$ and that D is unconditionally σ-invariant. It follows that either $D = H$, in which case $D \lhd N$, or else $\mathbf{N}_H(D) > D$. In the latter situation, $\mathbf{N}_N(D) \not\subseteq R$, and so $\mathbf{N}_N(D) > R$. Since $\mathbf{N}_N(D)$ is σ-invariant, it follows from the maximality of R that $\mathbf{N}_N(D) = N$. In either case, therefore, we have $D \lhd N$.

By Lemma 5.4, the action of σ on N/D is fixed-point free, and thus N/D is nilpotent and $R \lhd \lhd N$. Also, if $p = 2$, then N/D abelian, and each of its elements is inverted by σ. It follows in this case that R is σ-invariant. ∎

6. THEOREM B

We are finally ready to prove Theorem B, which we restate here.

(6.1) THEOREM. *Suppose that Q is a real field and that $Q \subseteq L$ is a repeated radical extension with $|L{:}Q|$ odd. If $Q \subseteq K \subseteq L$, then K is a repeated radical extension of Q.*

Proof. We can assume that $L \subseteq \mathbb{C}$, the complex numbers. Choose a Galois extension $E \supseteq Q$ with $L \subseteq E \subseteq \mathbb{C}$, and write $G = \mathrm{Gal}(E/Q)$. Since Q is real, E is invariant under complex conjugation and we let $\sigma \in G$ be the restriction of conjugation to E. Write $U = \mathrm{Gal}(E/L) \subseteq G$ and note that $|G{:}U| = |L{:}Q|$ is odd, and thus by Sylow's theorem, some conjugate U^τ of U in G contains σ. We can replace L by the Q-isomorphic field L^τ, and we can thus assume that $\sigma \in U$. (Note that the property of being a repeated radical extension of Q is preserved by Q-isomorphism.) Since $\sigma \in U$, we have $L \subseteq \mathbb{R}$, and in particular, L is quasireal and Theorem 3.1 applies.

Let $F \subseteq E$ be abelian over Q and contain all roots of unity in E, and write $N = \mathrm{Gal}(E/F)$ and $M = U \cap N$, as usual, so that there is an appropriate chain of subgroups for which the four conditions of Theorem 3.1 hold. We will show that K is a repeated radical extension of Q by verifying these conditions for K. We thus define $V = \mathrm{Gal}(E/K) \supseteq U$ and $R = V \cap N \supseteq M$, and we work with V and R in place of U and M.

By (i), we know that $|L \cap F{:}Q|$ is a power of 2. But $|L{:}Q|$ is odd, by hypothesis, and thus $L \cap F = Q$ and $K \cap F = Q$, and so (i) holds for the field K. Also $UN = G$ in this situation, and thus $|N{:}M| = |G{:}U| = |L{:}Q|$ is odd. We proceed to verify (ii), (iii), and (iv) for K.

Conditions (ii), (iii), and (iv) for L tells us that $M \lhd \lhd N$ and that there is a U-composition series $\mathscr{X}$ for N through M such that each factor of $\mathscr{X}$ above M is U-isomorphic to a group of roots of unity of prime order. As $|N{:}M|$ is odd, these primes are all odd, and thus complex conjugation acts fixed-point-freely on each of these groups of roots of unity. Since $\sigma \in U$, it follows that σ also acts fixed-point-freely on the factors of $\mathscr{X}$ above M, and Lemma 5.1 applies. We conclude that $R \lhd \lhd N$.

Now $R \lhd V$, and so by lemma 5.3, we can construct a V-invariant subnormal series from R to N, and this can be refined to a V-composition series $\mathscr{Y}$ for N that has R as one of its terms. Observe that $V = UR$ and, of course, R acts trivially on each of the factors of $\mathscr{Y}$ above R. These factors are therefore U-simple, and hence they are U-isomorphic to some of the factors above M in the U-composition series $\mathscr{X}$. In particular, each factor Y of $\mathscr{Y}$ above R is U-isomorphic to some subgroup $D \subseteq E^{\times}$ of prime order. Conditions (ii) and (iii) of Theorem 3.1 thus hold.

To complete the proof, it suffices to show that Y and D are actually V-isomorphic. But D consists of roots of unity, and so $D \subseteq F$ and N acts trivially on D. In particular, R acts trivially on D. Since R also acts trivially on Y and $V = UR$, it follows that Y and D are V-isomorphic, as required. ∎

7. THEOREM C

Let $f \in Q[X]$ be irreducible, where Q is a real field and f has at least one root that is contained in a real repeated radical extension of Q. By Theorem A, we know that only when $\deg(f)$ is a power of 2 can it be true that all of the complex roots of f are real. In the opposite extreme case, where $\deg(f)$ is odd, Theorem C asserts that f can have only the one real root with which we started. We are now ready to prove this.

Proof of Theorem C. We are given that f has a root α lying in some real repeated radical extension L of Q, and we choose a field E, Galois over Q, with $L \subseteq E \subseteq \mathbb{C}$. Let $F \subseteq E$ be abelian over Q and contain all roots of unity in E, and let G, U, N, and M have their usual meanings, so that the four conditions of Theorem 3.1 hold for an appropriate chain of subgroups. Note that f splits over E, and our task is thus to show that α is the only real root of f in E.

We argue first that it is no loss to assume that $L \cap F = Q$. To see why this is so, write $K = L \cap F$ and note that $Q[\alpha] \subseteq K[\alpha]$. It follows that $\deg(f) = |Q[\alpha]:Q|$ divides $|K[\alpha]:Q| = |K[\alpha]:K|\,|K:Q|$. Since $\deg(f)$ is odd and $|K:Q|$ is a power of 2 by the first condition of Theorem 3.1, we deduce that $\deg(f)$ divides $|K[\alpha]:K|$. It follows from this that f is irreducible over K. Since L is a real repeated radical extension of K, we can replace our ground field Q with K, leaving E and F unchanged. (Note that E is Galois over K and that F is abelian over K.) We can thus assume that $L \cap F = Q$, as claimed, and so we have $UN = G$.

Let $\beta \in E$ be a real root of f and recall that we must show that $\beta = \alpha$. Since $G = UN$ acts transitively on the roots of f in E and U fixes α (because $\alpha \in L$), there exists an element of N that carries α to β.

By Theorem 3.1, we have a U-invariant subnormal series $\mathscr{X}$ from M to N with factors U-isomorphic to prime-order subgroups of $E^{\times}$. Let X be the least term in $\mathscr{X}$ that contains an element τ carrying α to β. If $X = M$, then $\tau \in M \subseteq U = \mathrm{Gal}(E/L)$, and τ fixes $\alpha \in L$. In this case, $\beta = \alpha^{\tau} = \alpha$, as required. We can thus assume that $X > M$, and we let Y be the term just below X in the series $\mathscr{X}$. In particular, $M \subseteq Y \lhd X$ and X/Y is U-isomorphic to $\langle \epsilon \rangle$, where ϵ is a primitive pth root of unity in E for some prime p.

Now let $\sigma \in G$ be the restriction of complex conjugation to E and note that $\sigma \in U$ since L is real. Thus $X^{\sigma} = X$ and in particular, $\tau^{\sigma} \in X$ and $\tau^{\sigma}\tau^{-1} \in X$. Also, since β and α are both real, we compute that

$$\alpha^{\sigma\tau\sigma} = \alpha^{\tau\sigma} = \beta^{\sigma} = \beta = \alpha^{\tau}.$$

Thus $\tau^{\sigma}\tau^{-1}$ fixes α, and hence it lies in X_{α}, the stabilizer in X of α.

By the minimality of X, we see that no element of Y carries α to β, and thus we cannot have $X = X_{\alpha}Y$. Since $Y \lhd X$ has prime index, we deduce that $X_{\alpha} \subseteq Y$. We know, however, that $|G:G_{\alpha}| = \deg(f)$ is odd, and since $X \lhd\lhd G$, it follows that $|X:X_{\alpha}|$ is odd, and thus $|X/Y|$ is odd.

Since $\sigma \in U$ inverts the elements of $\langle \epsilon \rangle$, we deduce that σ inverts the elements of X/Y, and therefore no nonidentity element of X/Y is fixed by σ. But $\tau^{\sigma}\tau^{-1} \in X_{\alpha} \subseteq Y$, and this shows that the coset $Y\tau$ is a σ-fixed point of X/Y. We conclude that $\tau \in Y$, and this contradicts the choice of X. ∎

8. PRIME-POWER DEGREE EXTENSIONS

In this section we prove the following, which is Theorem E of the Introduction.

(8.1) THEOREM. *Let $Q \subseteq L$ be a repeated radical extension, where L is quasireal. If $|L:Q|$ is a prime power and $Q \subseteq K \subseteq L$, then K is a repeated radical extension of Q.*

We need the following easy lemma from group representation theory.

(8.2) LEMMA. *Let V be a finite group and suppose that $U \subseteq V$ is a subgroup, where $|V:U|$ is a power of a prime number p. Let X be a simple FV-module, where F has characteristic p, and suppose that all composition factors of X viewed as an FU-module are isomorphic and of dimension* 1. *Then* $\dim_F(X) = 1$.

Proof. Let R be a Sylow r-subgroup of U, where $r \neq p$. Then X is semisimple as an FR-module, and since $R \subseteq U$, all composition factors of this FR-module have dimension 1 and are isomorphic. It follows that each element of R acts via scalar multiplication on X.

Now let $Z \subseteq V$ be the subgroup consisting of all elements that act via scalar multiplication. We have seen that Z contains a full Sylow r-subgroup of U for each prime $r \neq p$, and since $|V:U|$ is a power of p, it follows that $|V:Z|$ is a power of p. Thus $V = PZ$, where P is some Sylow p-subgroup of V.

Now P fixes some nonzero element $x \in X$, and thus both P and Z stabilize the subspace $Fx \subseteq X$. Since $PZ = V$ and X is simple as an FV-module, we deduce that $Fx = X$ and the proof is complete. ∎

In the following, we use the standard group-theoretic notation $\mathbf{O}^p(N)$ for a finite group N. Recall that this is the unique smallest normal subgroup of N having p-power index, where p is a prime number. It is clear that $\mathbf{O}^p(N) \subseteq M$ whenever $M \lhd N$ and $|N:M|$ is a power of p. In fact, an easy inductive argument shows that $\mathbf{O}^p(N) \subseteq M$ whenever M is subnormal in N and has p-power index.

Proof of Theorem 8.1. To apply Theorem 3.1, let $E \supseteq L$ be Galois over Q and suppose that $F \subseteq E$ is abelian over Q and contains all roots of unity in E. As usual, write $G = \mathrm{Gal}(E/Q)$, $U = \mathrm{Gal}(E/L)$, $N = \mathrm{Gal}(E/F)$, and $M = U \cap N$ and note that the four conditions of Theorem 3.1 must hold since L is a repeated radical extension of Q. To show that K is a repeated radical extension of Q, we let $V = \mathrm{Gal}(E/K) \supseteq U$ and we write $R = V \cap N \supseteq M$. We must verify the four conditions of Theorem 3.1 in the situation where K replaces L, so that V replaces U and R replaces M.

Since $|K \cap F:Q|$ divides $|L \cap F:Q|$, which we are assuming is a power of 2, the first condition is satisfied for K, and we work toward proving (ii), (iii), and (iv).

Note that $|N:M| = |UM:U|$ divides $|G:U| = |L:Q|$, which is a power of some prime p. Since (iii) holds for the field L, we know that M is subnormal in N with p-power index, and it follows that $\mathbf{O}^p(N) \subseteq M \subseteq R \subseteq N$, and thus R is subnormal in N. Also R is V-invariant, and thus by Lemma 5.3, there exists a V-composition series $\mathscr{X}$ for N, having R as one of its terms. Let X be any one of the factors of $\mathscr{X}$ above R. To prove the three conditions we show that $|X| = p$ and that X is V-isomorphic to the subgroup $\langle \epsilon \rangle \subseteq E^{\times}$, where ϵ is a primitive pth root of unity in E.

Since $U \subseteq V$, we see that R is U-invariant, and the U-composition factors of N above R are among the U-composition factors of N above M. Each of these, however, is U-isomorphic to $\langle \epsilon \rangle$, and it follows that when X is viewed as a U-group, all of its composition factors are isomorphic and of order p. Since $|V:U|$ is a power of p, we can apply Lemma 8.2 to deduce that X has order p, and thus X is U-isomorphic to $\langle \epsilon \rangle$. But each p-element of V acts trivially on both X and $\langle \epsilon \rangle$, and since V is generated by U and p-elements, it follows that X and $\langle \epsilon \rangle$ are actually V-isomorphic, as required. ∎

9. EXAMPLES AND FURTHER REMARKS

Let Q be a real field and suppose that $f \in Q[X]$ is irreducible of degree n and that f has a root that lies in a real repeated radical extension of Q. By Theorem A, we know that if f has n real roots, then n must be a power of 2. To see that this actually can happen when n is an aribtrary power of 2, let p be any prime congruent to 1 modulo $2n$ and let E be the unique extension of degree n over $\mathbb{Q}$ contained in the cyclotomic field of pth roots of unity. Then E is a real field and $\mathrm{Gal}(E/\mathbb{Q})$ is a (cyclic) 2-group. It follows that E is a repeated radical extension of $\mathbb{Q}$, and so if we take f to be the minimal polynomial over $\mathbb{Q}$ of any generating element of E, we have the desired example.

If $n = \deg(f)$ is odd, on the other hand, then Theorem C tell us that f has only one real root. This suggests that perhaps in general, when n is not necessarily either odd or a power of 2, the number of real roots of f is at most the 2-part of n. This is incorrect, however, and we give an explicit example of an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree 6 having four real roots, of which exactly one lies in a real repeated radical extension of $\mathbb{Q}$. (This also shows that not all real roots of an irreducible polynomial over $\mathbb{Q}$ need be "alike": it is possible for some to lie in real repeated radical extensions while others do not.)

We claim that the polynomial $f(X) = (X^3 - 3X + 3)^2 - 3$ has the desired properties. First, note that f is irreducible over $\mathbb{Q}[X]$ by the Eisenstein criterion since the constant term of f is 6, the leading coefficient is 1, and all of the other coefficients are divisible by 3. Next, we factor $f(X) = (X^3 - 3X + 3 + \sqrt{3})(X^3 - 3X + 3 - \sqrt{3})$, and we investigate the (complex) roots of each factor.

Let x be a real variable and consider the polynomial function $h(x) = x^3 - 3x + a$, where a is a real number. Since h has a local maximum at $x = -1$ and a local minimum at $x = 1$, we see that the graph of $y = h(x)$ meets the x-axis as many as three times if and only if $h(-1) > 0$ and $h(1) < 0$. Since $h(-1) = a + 2$ and $h(1) = a - 2$, it follows that the condition for h to have three real zeros is that $-2 < a < 2$. (This can also be checked by considering the discriminant of h.) The number $a = 3 - \sqrt{3}$ clearly satisfies this condition, but $a = 3 + \sqrt{3}$ does not. Returning now to the factors of the polynomial $f(X)$, we deduce that $u(X) = X^3 - 3X + 3 + \sqrt{3}$ has exactly one real root while $v(X) = X^3 - 3X + 3 - \sqrt{3}$ has three real roots. Therefore, $f(X)$ has a total of four real roots, as claimed.

Next, we observe that each of the polynomials u and v is irreducible over $\mathbb{Q}[\sqrt{3}]$ since otherwise, one of these polynomials, and therefore also f, would have a root in this quadratic extension of $\mathbb{Q}$, and this is impossible since f is irreducible of degree 6 over $\mathbb{Q}$. By Theorem A, therefore, none of the three real roots of v lies in a real repeated radical extension of $\mathbb{Q}[\sqrt{3}]$, and thus none lies in a real repeated extension of $\mathbb{Q}$.

What remains is to show that the unique real root of u does lie in a real repeated radical extension of $\mathbb{Q}$, and for this purpose, it suffices to show that it lies in a real repeated radical extension of $\mathbb{Q}[\sqrt{3}]$. The following result does the job.

(9.1) THEOREM. *Let Q be a real field and suppose that $f \in Q[X]$ is an irreducible cubic polynomial having exactly one real root α. Then α lies in a real repeated radical extension of Q.*

Note that the converse of Theorem 9.1 is also true: if the irreducible cubic polynomial f has a root α that lies in a real repeated radical extension of Q, then α is the only real root of f. This case of Theorem C also follows by Theorem A, since if a real cubic polynomial has two real roots, it has three.

Actually, something slightly more general than Theorem 9.1 is true, and so we state this improved result and prove it instead.

(9.2) THEOREM. *Let Q be a real field and suppose that $f \in Q[X]$ is a solvable irreducible polynomial of degree p over Q, where p is a Fermat prime. If f does not split over $\mathbb{R}$, then f has a root that lies in a real repeated radical extension of Q.*

Proof. Let S be the splitting field for f over Q in $\mathbb{C}$ and let $H = \mathrm{Gal}(S/Q)$, so that H is a solvable permutation group of prime degree p. It is well known and easy to prove that H must have a normal subgroup P of order p and that H/P is isomorphic to a subgroup of the abelian group $\mathrm{Aut}(P)$, which in our case, where p is Fermat, has 2-power order. It follows that there exists a field T with $Q \subseteq T \subseteq S$, such that T is abelian over Q, and where $|S:T| = p$, and $|T:Q|$ is a power of 2.

Next, we define $E = S[\epsilon]$, where ϵ is a complex primitive pth root of unity. (It is possible, of course, that $\epsilon \in S$, in which case $E = S$.) Note that $Q[\epsilon]$ is Galois over Q of degree dividing $p - 1$, which is a power of 2. Since $E = SQ[\epsilon]$ is a compositum of Galois extensions of Q, we see that E is Galois over Q. Also, by the natural irrationalities theorem, $|E:S|$ divides $|Q[\epsilon]:Q|$ and we see that $|E:Q| = 2^e p$, for some integer e.

The restriction of complex conjugation to E is an element σ of $G = \mathrm{Gal}(E/Q)$, and we write $U = \langle \sigma \rangle$ and $L = E \cap \mathbb{R}$, so that $\mathrm{Gal}(E/L) = U$. Since $\deg(f) = p$ is odd, f has some real root α, and we have $\alpha \in L$. We are assuming that f does not split over $\mathbb{R}$, and in particular, it does not split over L and L is not Galois over Q. It follows that U is not normal in G, and thus U is nontrivial, so that $|U| = 2$.

We propose to complete the proof by appealing to Theorem 3.1 to show that L is a repeated radical extension of Q. For this purpose, we need a field $F \subseteq E$ that is abelian over Q and contains all roots of unity in E. Because T is abelian over Q, it follows by Lemma 2.4 that we can choose F so that it contains T. (Actually, it is not hard to see that we can take $F = T[\epsilon]$, but we shall not need that fact.) Now $\mathrm{Gal}(F/Q)$ is abelian, and thus if $\alpha \in F$, the polynomial f would split over the real field $Q[\alpha]$. This is contrary to the hypothesis, and therefore, $\alpha \notin F$. Thus $T \subseteq F \cap S < S$, and since $|S:T| = p$ is prime, we deduce that $F \cap S = T$. Also, $\epsilon \in F$, and thus $SF = E$, and we conclude by the natural irrationalities theorem that $|E:F| = |S:T| = p$. Writing $N = \mathrm{Gal}(E/F)$, as usual, we see that $|N| = p$.

We are now ready to check the four conditions of Theorem 3.1. Since $N \lhd G$ has order p and $|U| = 2$, we see that $|UN| = 2p$. Thus $|F \cap L:Q| = |G:UN|$, and this is a power of 2 because $|G| = 2^e p$. This verifies the first condition of Theorem 3.1.

Next, observe that $M = U \cap N$ is trivial, and since $|N| = p$, the second and third conditions hold for the subgroup chain $M \subseteq N$. To verify the fourth condition, we need to show that N is U-isomorphic to $\langle \epsilon \rangle$. The unique nonidentity element σ of U inverts the elements of $\langle \epsilon \rangle$, and so it suffices to show that U acts nontrivially on N. (The only possible nontrivial action of U on the group N of prime order is for the involution in U to invert all elements of N.) In other words, it is enough to establish that U is not normal in UN. Observe that $UN \lhd G$ since $G/N \cong \mathrm{Gal}(F/Q)$ is abelian. If $U \lhd UN$, then U would be characteristic in UN, and hence $U \lhd G$. We know that this is not the case, however, and this completes the proof. ∎

This completes the argument that the sixth degree irreducible polynomial over $\mathbb{Q}$ that we described previously does indeed have exactly four real roots and that exactly one of them is in a real repeated radical extension of $\mathbb{Q}$.

An obvious question at this point is whether or not the hypothesis that p is a Fermat prime is really necessary in Theorem 9.2. Although we have not found an explicit example, it seems likely that the conclusion of Theorem 9.2 does not hold more generally.

In the situation of Theorem 9.1, we know that α lies in a real repeated radical extension of Q, but it is not necessarily the case that the cubic extension $Q \subseteq Q[\alpha]$ is radical (and when it is not radical, it is obviously not a repeated radical extension either). This shows that, in general, subfields of real repeated radical extensions of a real field Q need not be repeated radical extensions of Q. In fact, an example exists over the rational numbers $\mathbb{Q}$.

(9.3) EXAMPLE. There exists an irreducible cubic polynomial over $\mathbb{Q}$ having a unique real root α, where $\mathbb{Q}[\alpha]$ is not a repeated radical extension of $\mathbb{Q}$. In fact, the polynomial $X^3 - 3X + 3$ has this property.

The construction for Example 9.3 relies on the following easy result.

(9.4) THEOREM. *Let $f \in Q[X]$ be an irreducible cubic polynomial, where Q is a quasireal field. Suppose that α is a root of f in some extension field of Q and that $Q[\alpha]$ is a repeated radical extension of Q. Then the discriminant of f is $-3m^2$ for some element $m \in Q$.*

Proof. Let S be a splitting field for f over Q and let Δ be the discriminant of f. Since $|Q[\alpha]:Q| = 3$, we see that $Q[\alpha]$ must actually be a radical extension of Q, and so by Lemma 2.1(c), we know that $Q[\alpha] = Q[\beta]$, where $\beta^3 \in Q$. The polynomial $X^3 - \beta^3$ is thus irreducible in $Q[X]$, and hence it splits over S. It follows that S contains the primitive cube root of unity $\omega = (-1 + \sqrt{-3})/2$, and so in particular, it contains $\sqrt{-3}$, and -3 is a square in S. Also, since Q is quasireal, $\omega \notin Q$, and thus $\mathrm{Gal}(S/Q)$ has order 6 and is isomorphic to the full symmetric group of degree 3. It follows that Δ is not a square in Q. In this case, S contains a unique quadratic extension T of Q and T is Galois over Q. Each of $\sqrt{\Delta}$ and $\sqrt{-3}$ must lie in T and each of these elements is negated by the unique nonidentity automorphism in $\mathrm{Gal}(T/Q)$. It follows that $\sqrt{\Delta}/\sqrt{-3}$ is fixed by $\mathrm{Gal}(T/Q)$, and it hence lies in Q. In other words, $\Delta/(-3)$ is a square in Q, as desired. ∎

Proof of Example 9.3. Let $f(X) = X^3 - 3X + 3 \in \mathbb{Q}[X]$, so that f is irreducible by the Eisenstein criterion. Also, since the constant term of f does not lie between -2 and 2, we know by our earlier analysis that f must have exactly one real root α.

Recall that the discriminant Δ of the polynomial $X^3 + bX + c$ is $-4b^3 - 27c^2$. (See the discussion following Lemma 23.21 in [2], for example.) In our case, where $b = -3$ and $c = 3$, we compute that $\Delta(f) = -(5)(27)$, and this is not of the form $-3m^2$ with $m \in \mathbb{Q}$. It follows by Theorem 9.4 that $Q[\alpha]$ cannot be a repeated radical extension of $\mathbb{Q}$. ∎

There is an analog of Theorem 9.1 for quartic polynomials. Although this result too can be proved using Theorem 3.1, we have decided to use an alternative approach.

(9.5) THEOREM. *Let Q be a real field and suppose that $f \in Q[X]$ is an irreducible quartic polynomial having exactly two real roots. Then each real root of f lies in a real repeated radical extension of Q.*

Proof. Let α, β, γ, and δ be the four (distinct) complex roots of f, where α and β are real and γ and δ are nonreal complex conjugates. Define the complex numbers $r = \alpha\beta + \gamma\delta$, $s = \alpha\gamma + \beta\delta$, and $t = \alpha\delta + \beta\gamma$, and observe that r is real and that s and t are distinct since $s - r = (\alpha - \beta)(\gamma - \delta) \neq 0$. Also, s and t are complex conjugates, and so they are nonreal.

We claim that r is contained in some real repeated radical extension L of Q. To see why this is so, observe that the Galois group of f over Q permutes the set $\{r, s, t\}$. This group thus fixes the coefficients of the polynomial $g(X) = (X - r)(X - s)(X - t)$, and we deduce that $g \in Q[X]$. If g is reducible over Q, then $|Q[r]:Q| \leq 2$, and in this case, $Q[r]$ is a radical extension of Q and we can take $L = Q[r]$. Otherwise, g is irreducible over Q, and since r is the unique real root of g, it follows that L exists by Theorem 9.1.

Let $u = \alpha\beta\gamma\delta$ and observe that $u \in Q \subseteq L$. We compute that $r\alpha\beta = (\alpha\beta)^2 + u$, and thus $\alpha\beta$ satisfies a quadratic equation over L. Thus $L[\alpha\beta]$ is a real field of degree at most 2 over L, and hence it is a real repeated radical extension of Q. Replacing L by $L[\alpha, \beta]$, therefore, we can assume that $\alpha\beta \in L$.

Now let $v = \alpha + \beta + \gamma + \delta \in Q \subseteq L$. Then

$$\begin{aligned}(\alpha + \beta)(v - (\alpha + \beta)) &= (\alpha + \beta)(\gamma + \delta) \\ &= s + t = (r + s + t) - r \in L,\end{aligned}$$

since $r + s + t \in Q$. Thus $\alpha + \beta$ satisfies a quadratic equation over L, and reasoning as before, we can replace L by $L[\alpha + \beta]$ and assume that

$\alpha + \beta \in L$. Finally, since $\alpha\beta$ and $\alpha + \beta$ each lie in L, we see that $|L[\alpha]:L| \leq 2$, and thus α and β lie in the real repeated radical extension $L[\alpha]$ of Q. ∎

Finally, we want to show that the hypothesis in Theorem B that Q is real cannot be removed.

(9.6) EXAMPLE. There exist fields $Q \subseteq K \subseteq L \subseteq \mathbb{C}$, where L is a repeated radical extension of Q and $|L:Q|$ is odd, but where K is not a repeated radical extension of Q.

Proof. Let $L = \mathbb{Q}[\epsilon]$, where ϵ is a primitive complex 19th root of unity, so that $|L:\mathbb{Q}| = 18$. Let Q be the unique quadratic extension of $\mathbb{Q}$ in L and let K be the unique field of degree 3 over Q in L. Now $L = Q[\epsilon]$ is a radical extension of Q of degree 9 and we claim that the cubic extension $Q \subseteq K$ is not a repeated radical extension. It suffices, of course, to show that K is not a radical extension of Q.

The only roots of unity in L are the 38th roots of unity, and thus the only roots of unity in K are ± 1. We know that K is Galois over Q since $\mathrm{Gal}(L/Q)$ is abelian, and since $|K:Q| = 3$, we see by lemma 2.3(a) that K cannot be radical over Q. ∎

ACKNOWLEDGMENTS

We acknowledge the contribution of H. W. Lenstra, Jr., who first suggested Theorem B as a problem and who provided the statement and proof of Theorem D. Part of this paper is part of the Ph.D. thesis of the second author, written under Lenstra's supervision at the University of California, Berkeley. Also, the first author is grateful to the University of California for its hospitality while he was visiting there, on sabbatical from the University of Wisconsin, Madison.

REFERENCES

1. I. M. Isaacs, Solutions of polynomials by real radicals, *Amer. Math. Monthly* **92** (1985), 571–575.
2. I. M. Isaacs, "Algebra: A Graduate Course," Brooks/Cole, Pacific Grove, CA, 1994.