PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 11, November 2007, Pages 3435–3441
S 0002-9939(07)08864-8
Article electronically published on August 1, 2007

RADICAL AND CYCLOTOMIC EXTENSIONS OF THE RATIONAL NUMBERS

DAVID GLUCK AND I. M. ISAACS

(Communicated by Martin Lorenz)

ABSTRACT. A radical extension of the rational numbers $\mathbb{Q}$ is a field $R \supseteq \mathbb{Q}$ generated by an element having a power in $\mathbb{Q}$, and a cyclotomic extension $K \supseteq \mathbb{Q}$ is an extension generated by a root of unity. We show that a radical extension that is almost Galois over $\mathbb{Q}$ is almost cyclotomic. More precisely, we prove that if R is radical with Galois closure E, then E contains a cyclotomic field K such that the degree $|E : K|$ is bounded above by an almost linear function of $|E : R|$. In particular, if R is Galois, it contains a cyclotomic field K such that $|R : K| \leq 3$.

1. INTRODUCTION

Recall that a *radical extension* of a field F is a field $R \supseteq F$ such that $R = F[\alpha]$ for some element $\alpha \in R$ having a power in the ground field F. (Note that there is a notational ambiguity in the literature. We distinguish radical extensions from *repeated radical extensions*, which are towers of radical extensions, and which are central to Galois' theorem on solvability of polynomials. Repeated radical extensions are not relevant to this paper.)

Let $R = F[\alpha]$, where $\alpha^n = a \in F$, and observe that all roots of the polynomial $X^n - a$ in every extension field of R have the form $\alpha\epsilon$, where ϵ is some nth root of unity. In particular, since the minimal polynomial of α over F divides $X^n - a$, all of its roots have this form. It is thus clear that there is a close connection between radical extensions and roots of unity, and our goal is to explore this connection for radical extensions of the rational numbers $\mathbb{Q}$. For this purpose, it is no loss to limit our attention to fields contained in the complex numbers $\mathbb{C}$, and so all fields we consider are assumed to be subfields of $\mathbb{C}$.

By a *cyclotomic* field, we mean one of the fields $\mathbb{Q}_n$, generated by the nth roots of unity in $\mathbb{C}$, where n is a positive integer. It is clear that the field generated by two cyclotomic fields $\mathbb{Q}_n$ and $\mathbb{Q}_m$ is again cyclotomic (and in fact, it is $\mathbb{Q}_k$, where k is the least common multiple of n and m). It follows that every finite degree extension E of $\mathbb{Q}$ contains a unique largest cyclotomic field K, and every root of unity in E lies in K.

Our main result is essentially that a radical extension of $\mathbb{Q}$ that is close to being Galois over $\mathbb{Q}$ cannot be far from being cyclotomic. A more precise statement is the following, in which as usual, φ denotes Euler's totient function.

Received by the editors July 5, 2006.
2000 *Mathematics Subject Classification.* Primary 12F10.

Theorem A. *Let R be a radical extension of $\mathbb{Q}$. Let E be the Galois closure of R over $\mathbb{Q}$, and let K be the maximum cyclotomic field contained in E. Writing $c = |E : R|$ and $m = |E : K|$, we have $\varphi(m) \leq 2c$, and if m is even, then $\varphi(m) \leq c$. There exists, therefore, an upper bound on m in terms of c.*

In particular, consider a radical extension of $\mathbb{Q}$ that actually is Galois over $\mathbb{Q}$.

Corollary B. *Let R be a radical extension of $\mathbb{Q}$, and assume that R is Galois over $\mathbb{Q}$. Then $|R : K| \leq 3$, where K is the maximum cyclotomic field contained in R.*

Proof. We are in the situation of Theorem A with $c = 1$, and thus if $m = |R : K|$, we have $\varphi(m) \leq 2$ and $\varphi(m) = 1$ if m is even. The set of integers m with $\varphi(m) = 1$ is $\{1, 2\}$ and the corresponding set for $\varphi(m) = 2$ is $\{3, 4, 6\}$. Since 3 is the only odd member of the latter set, the result follows. □

Of course, every cyclotomic field is both Galois and radical over $\mathbb{Q}$, and thus it is certainly possible to have $|R : K| = 1$ in Corollary B. We shall see that there are also examples with $|R : K| = 2$ and $|R : K| = 3$, and so Corollary B is sharp. For Theorem A, we show at least that our bounds have the right order of magnitude. Specifically, we construct examples where m is an arbitrary odd integer and $\varphi(m) = c$.

Finally, we consider the following question. Given an extension E of $\mathbb{Q}$ that we know to be Galois, how can we determine whether or not it is radical? (This seems more interesting and more difficult than the reverse question of deciding whether or not a visibly radical extension is Galois.) Of course, Corollary B provides a necessary condition: we must have $|E : K| \leq 3$, where as usual K is the maximum cyclotomic field in E. It seems harder to find a sufficient condition, however. We explore this by considering extensions E of $\mathbb{Q}$ that are splitting fields for polynomials of the form $X^4 - k$, where k is a square-free integer and $|k| > 1$. We will show that among these fields, E is radical over $\mathbb{Q}$ if and only if $k = \pm 3$.

2. Theorem A

We begin work toward a proof of Theorem A with an easy observation. If $F \subseteq E$ are fields, and $\alpha \in E$ is an element such that $\alpha^m \in F$ and $\alpha^n \in F$ for positive integers m and n, then $\alpha^d \in F$, where $d = (m, n)$, the greatest common divisor. To see this, write $d = km + ln$, where k and l are (not necessarily positive) integers. Since we can certainly assume that $\alpha \neq 0$, we can write $\alpha^d = (\alpha^m)^k(\alpha^n)^l$, and so $\alpha^d \in F$, as wanted. It follows that if n is the smallest positive integer such that $\alpha^n \in F$, then $d = n$, and thus n divides m.

We need several elementary lemmas.

Lemma 2.1. *Let $R = \mathbb{Q}[\alpha]$, where $\alpha^n \in \mathbb{Q}$ and n is the smallest positive integer with this property, and let E be the Galois closure of R over $\mathbb{Q}$. Then E contains a primitive nth root of unity.*

Proof. Let t be the order of the (necessarily finite) group of roots of unity in E. If $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, then α^σ is a root of the minimal polynomial of α over $\mathbb{Q}$, and so we can write $\alpha^\sigma = \alpha\epsilon$ for some root of unity ϵ. Of course, $\epsilon \in E$, and thus $\epsilon^t = 1$. We have $(\alpha^t)^\sigma = \alpha^t\epsilon^t = \alpha^t$ for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, and thus α^t is rational. It follows by the minimality of n that n divides t, and thus since the group of roots of unity in E is cyclic, it contains an element of order n, as wanted. □

In the situation of Lemma 2.1, we know that the maximum cyclotomic subfield K of E contains a primitive nth root of unity. Also, $E = K[\alpha]$ and $\alpha^n \in K$. It follows by a standard result of elementary Galois theory that $\mathrm{Gal}(E/K)$ is cyclic. (This is the easier half of Theorem 22.8 of [2].) We shall not need this fact, however.

Lemma 2.2. *Let $R = \mathbb{Q}[\alpha]$, where $\alpha^n \in \mathbb{Q}$, and let E be the Galois closure of R over $\mathbb{Q}$. Write $m = |E : K|$, where K is the maximum cyclotomic subfield of E. Then $|R : K \cap R| = m$ and $K \cap R = \mathbb{Q}[\alpha^m]$.*

Proof. All roots of the minimal polynomial f of α over $\mathbb{Q}$ have the form $\alpha\epsilon$, where $\epsilon \in E$ is a root of unity, and hence $\epsilon \in K$. It follows that f splits over $K[\alpha]$, and thus $K[\alpha] = E$. Now let g be the minimal polynomial of α over K, and observe that g has degree m since $E = K[\alpha]$ and $|E : K| = m$. The constant term of g is plus or minus the product of the m roots of g, each of which has the form $\alpha\epsilon$, where $\epsilon \in K$. Since the constant term itself lies in K, it follows that $\alpha^m \in K$, and we have $\alpha^m \in K \cap R$.

Now $R = (K \cap R)[\alpha]$ and $E = K[\alpha]$, and thus since the minimal polynomial of α over $K \cap R$ has coefficients in K, we have $|R : K \cap R| \geq |E : K|$. Therefore,

$$m = |E : K| \leq |R : K \cap R| \leq |R : \mathbb{Q}[\alpha^m]| \leq m\,,$$

where the last inequality follows because $R = \mathbb{Q}[\alpha]$ and α is a root of a polynomial of degree m over $\mathbb{Q}[\alpha^m]$. It follows that $|R : K \cap R| = m$ and $K \cap R = \mathbb{Q}[\alpha^m]$, as required. □

Lemma 2.3. *Let $E \supseteq \mathbb{Q}$ be a Galois extension such that $\mathrm{Gal}(E/\mathbb{Q})$ is abelian, and let $\alpha \in E$ be an element such that $\alpha^n \in \mathbb{Q}$ for some positive integer n. Write $r = |\alpha|^2$. Then r is a positive rational number, and $\alpha = \delta\sqrt{r}$ for some $(2n)$th root of unity δ.*

Proof. Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Then $(\alpha^\sigma)^n = (\alpha^n)^\sigma = \alpha^n$, and so $|\alpha^\sigma|^n = |\alpha|^n$, and we conclude that $|\alpha^\sigma| = |\alpha|$. Also, since E is Galois over $\mathbb{Q}$, complex conjugation maps E to itself, and the restriction of complex conjugation to E is a member of $\mathrm{Gal}(E/\mathbb{Q})$. We are assuming that this Galois group is abelian, however, and so we have $(\overline{\alpha})^\sigma = \overline{\alpha^\sigma}$ for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Thus

$$(|\alpha|^2)^\sigma = (\alpha\overline{\alpha})^\sigma = \alpha^\sigma\overline{\alpha}^\sigma = \alpha^\sigma\overline{\alpha^\sigma} = |\alpha^\sigma|^2 = |\alpha|^2\,,$$

and it follows that $|\alpha|^2$ is rational, and, of course, it is positive. Since $(\alpha^\sigma)^n = \alpha^n$ for every element $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, we have $(\overline{\alpha})^n = \alpha^n$. Then

$$1 = (\alpha/\overline{\alpha})^n = (\alpha^2/\alpha\overline{\alpha})^n = (\alpha^2/|\alpha|^2)^n = (\alpha/\sqrt{r})^{2n}\,,$$

where $r = |\alpha|^2$. Thus $\delta = \alpha/\sqrt{r}$ is a $(2n)$th root of unity, as wanted. □

It is interesting to compare the following with Corollary B. Both here and in that corollary, we consider radical extensions R of $\mathbb{Q}$ that are Galois over $\mathbb{Q}$. Recall that Corollary B asserts that there exists a cyclotomic subfield K of R such that $|R : K| \leq 3$. Here, we add the hypothesis that the Galois group is abelian, and we get the stronger conclusion that $|R : K| \leq 2$, where K is a specific cyclotomic field.

Corollary 2.4. *Let $R = \mathbb{Q}[\alpha]$, where $\alpha^n \in \mathbb{Q}$ and n is the smallest positive integer with this property. Assume that R is Galois over $\mathbb{Q}$ and that $\mathrm{Gal}(R/\mathbb{Q})$ is abelian. Then $\mathbb{Q}_n \subseteq R$ and $|R : \mathbb{Q}_n| \leq 2$. Also, if n is odd, then $R = \mathbb{Q}_n$.*

Proof. We have $\mathbb{Q}_n \subseteq R$ by Lemma 2.1. Also, $\alpha^2 \in \mathbb{Q}_n$ since by Lemma 2.3 we can write $\alpha^2 = r\epsilon$, where r is rational and ϵ is an nth root of unity. It follows that $|R : \mathbb{Q}_n| = |\mathbb{Q}_n[\alpha] : \mathbb{Q}_n| \leq 2$, as wanted. Since $\alpha^2 \in \mathbb{Q}_n$ and $\alpha^n \in \mathbb{Q} \subseteq \mathbb{Q}_n$, we have $\alpha^d \in \mathbb{Q}_n$, where $d = (2, n)$. In particular, if n is odd, then $\alpha \in \mathbb{Q}_n$, and so $R = \mathbb{Q}_n$. □

Lemma 2.5. *Let x and y be positive integers. Then $\varphi(x)\varphi(y) \leq \varphi(xy)$, and if both x and y are even, then $2\varphi(x)\varphi(y) \leq \varphi(xy)$.*

Proof. Since φ is a multiplicative function, it suffices to establish the result in the case where both x and y are powers of some prime p. Also, since there is nothing to prove if $x = 1$ or if $y = 1$, we can assume that both x and y are proper powers of p. Then $\varphi(x) = x(p-1)/p$ and similarly for y and for xy. Thus

$$\varphi(x)\varphi(y) \leq \left(\frac{p}{p-1}\right)\varphi(x)\varphi(y) = \left(\frac{p}{p-1}\right)\frac{xy(p-1)^2}{p^2} = \left(\frac{p-1}{p}\right)xy = \varphi(xy)\,,$$

as wanted. The final assertion follows because $p/(p-1) = 2$ when $p = 2$. □

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

Theorem A. *Let R be a radical extension of $\mathbb{Q}$. Let E be the Galois closure of R over $\mathbb{Q}$, and let K be the maximum cyclotomic field contained in E. Writing $c = |E : R|$ and $m = |E : K|$, we have $\varphi(m) \leq 2c$, and if m is even, then $\varphi(m) \leq c$. There exists, therefore, an upper bound on m in terms of c.*

Proof. Write $R = \mathbb{Q}[\alpha]$, where $\alpha^n \in \mathbb{Q}$ for some positive integer n, and suppose that n is as small as possible. Let $S = K \cap R$, and observe that $|R : S| = m$ and $S = \mathbb{Q}[\alpha^m]$ by Lemma 2.2. Also, $m|K : S| = |E : S| = c|R : S| = cm$, and so $|K : S| = c$.

Since $\alpha^n \in \mathbb{Q} \subseteq S$ and $\alpha^m \in S$, it follows that $\alpha^d \in S$, where $d = (m, n)$. Then $m = |R : S| \leq |R : \mathbb{Q}[\alpha^d]| \leq d$, and since d divides m, we have $d = m$, and thus m divides n. Set $l = n/m$ so that $n = ml$, and hence $\varphi(m) \leq \varphi(n)/\varphi(l)$ by Lemma 2.5. Also by Lemma 2.5, if both m and l are even, then $2\varphi(m) \leq \varphi(n)/\varphi(l)$.

Write $\beta = \alpha^m$, so that we have $S = \mathbb{Q}[\beta]$. Also $\beta^l \in \mathbb{Q}$, and l is the smallest positive integer with this property. Since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian and $S \subseteq K$, it follows that S is Galois over $\mathbb{Q}$ and that $\mathrm{Gal}(S/\mathbb{Q})$ is abelian, and so Corollary 2.4 applies. We conclude that $\mathbb{Q}_l \subseteq S$ and that $|S : \mathbb{Q}_l| \leq 2$. Furthermore, if l is odd, then $S = \mathbb{Q}_l$.

Since $|K : S| = c$, we have $|K : \mathbb{Q}_l| \leq 2c$, and if l is odd, $|K : \mathbb{Q}_l| = c$. Also, $\mathbb{Q}_n \subseteq E$ by Lemma 2.1, and thus $\mathbb{Q}_l \subseteq \mathbb{Q}_n \subseteq K$. Then $|\mathbb{Q}_n : \mathbb{Q}_l| \leq 2c$ and $|\mathbb{Q}_n : \mathbb{Q}_l| \leq c$ if l is odd. This yields

$$\varphi(m) \leq \frac{\varphi(n)}{\varphi(l)} = \frac{|\mathbb{Q}_n : \mathbb{Q}|}{|\mathbb{Q}_l : \mathbb{Q}|} = |\mathbb{Q}_n : \mathbb{Q}_l| \leq 2c\,,$$

as wanted. Also, in the case where l is odd or where both l and m are even, we have $\varphi(m) \leq c$. This inequality, therefore, always holds if m is even.

Finally, it is easy to see that $m \leq \varphi(m)^2$ if m is odd, and that $m \leq 2\varphi(m)^2$ in general. This yields $m \leq 4c^2$ in all cases, and so m is bounded in terms of c, as required. In fact, we can obtain a much better order of magnitude estimate by appealing to Theorem 328 in Hardy and Wright [1]. According to that result, there is some constant A such that $\varphi(m) > Am/\log(\log(m))$ for all $m > 1$. Since

$m < 4c^2$, we see that $\log(\log(m))$ is at most a constant multiple of $\log(\log(c))$, and since $\varphi(m) \leq 2c$, we deduce that m is bounded above by a constant multiple of $c\log(\log(c))$. □

3. Examples

We show first that the inequality $\varphi(m) \leq 2c$ of Theorem A is of the right order of magnitude, at least when m is odd. In fact, for every odd integer m, it is easy to construct examples where $\varphi(m) = c$.

Theorem 3.1. *Given an odd positive integer n and a prime p, write $\alpha = \sqrt[n]{p}$. Let $R = \mathbb{Q}[\alpha]$, so that R is radical over $\mathbb{Q}$. Define fields E and K and integers m and c as in Theorem A. Then $m = n$ and $c = \varphi(n)$.*

In fact more is true, which we will not prove. The assumption that p is prime can be weakened, and there are cases where one can compute m and c fairly easily even when n is not odd.

Proof of Theorem 3.1. Write $S = K \cap R$ and apply Lemma 2.2 to get $S = \mathbb{Q}[\alpha^m]$. Now α^m is a root of the polynomial $X^n - p^m$, and thus $(\alpha^m)^\sigma$ is also a root of this polynomial for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Furthermore, since $S \subseteq K$ and $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, it follows that S is Galois over $\mathbb{Q}$, and thus $(\alpha^m)^\sigma \in S$.

Since α^m is real, $S = \mathbb{Q}[\alpha^m]$ is a real field, and hence $(\alpha^m)^\sigma$ is also real. But n is odd, so the polynomial $X^n - p^m$ has a unique real root, and we have $(\alpha^m)^\sigma = \alpha^m$ for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Then $\alpha^m \in \mathbb{Q}$, and so $S = \mathbb{Q}[\alpha^m] = \mathbb{Q}$.

The polynomial $X^n - p$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. Then $|R : \mathbb{Q}| = n$, and so n is the smallest positive integer such that α^n is rational, and, in particular, $n \leq m$. Also, we can apply Lemma 2.1 to get $\mathbb{Q}_n \subseteq E$, and thus $\mathbb{Q}_n \subseteq K$. Since $X^n - p$ splits over $\mathbb{Q}_n[\alpha]$, we have $\mathbb{Q}_n[\alpha] = E$, and thus

$$n \leq m = |E : K| \leq |E : \mathbb{Q}_n| = |\mathbb{Q}_n[\alpha] : \mathbb{Q}_n| \leq n\,.$$

Then $|E : \mathbb{Q}_n| = n = m$, and

$$cn = c|R : \mathbb{Q}| = |E : \mathbb{Q}| = |E : \mathbb{Q}_n||\mathbb{Q}_n : \mathbb{Q}| = n\varphi(n)\,.$$

Thus $c = \varphi(n)$ and the proof is complete. □

Next we consider the situation where a field R is both radical and Galois over $\mathbb{Q}$. Recall that the assertion of Corollary B is that $m \leq 3$ in this case, and by Lemma 2.4 we know that $m \leq 2$ if $\mathrm{Gal}(R/\mathbb{Q})$ is abelian. It is trivial to see that we really can have $m = 2$; simply take $R = \mathbb{Q}[\sqrt{p}]$, where p is a prime number.

The following shows that $m = 3$ is also possible in Corollary B.

Example 3.2. There exists a radical extension $R \supseteq \mathbb{Q}$ such that R is Galois over $\mathbb{Q}$ and $|R : K| = 3$, where K is the maximum cyclotomic subfield of R.

Proof. Let R be the splitting field of $X^3 - 2$ over $\mathbb{Q}$, so that R is Galois over $\mathbb{Q}$, and as is well known, $|R : \mathbb{Q}| = 6$. To see that R is radical over $\mathbb{Q}$, we show that $R = \mathbb{Q}[\alpha]$, where $\alpha = i\sqrt{3}\sqrt[3]{2}$, and hence $\alpha^6 \in \mathbb{Q}$. Since $i\sqrt{3} \in \mathbb{Q}_3 \subseteq R$, it is clear that $\alpha \in R$. Also, $\mathbb{Q}[\alpha^2] = \mathbb{Q}[\sqrt[3]{2}]$, and R has degree 2 over this real field. Since α is nonreal, we have $\mathbb{Q}[\alpha] > \mathbb{Q}[\alpha^2]$, and thus $\mathbb{Q}[\alpha] = R$, as wanted. Finally, since the Galois group of R over $\mathbb{Q}$ is nonabelian, we have $\mathbb{Q}_3 \subseteq K < R$. But $|R : \mathbb{Q}_3| = 3$, and it follows that $K = \mathbb{Q}_3$ and $|R : K| = 3$. □

We have just seen that the splitting field of $X^3 - 2$ over $\mathbb{Q}$ is radical over $\mathbb{Q}$, although perhaps not obviously so. In a similar vein, we show that the splitting fields of $X^4 + 3$ and $X^4 - 3$ over $\mathbb{Q}$ are radical over $\mathbb{Q}$. Observe that these provide examples with nonabelian Galois groups where $m = 2$ in Corollary B. (It suffices to show that $m \neq 1$ and $m \neq 3$, and these assertions follow from the well-known facts that these splitting fields have degree 8 over $\mathbb{Q}$ and that their Galois groups are nonabelian.)

Lemma 3.3. *The splitting fields of $X^4 - 3$ and $X^4 + 3$ over $\mathbb{Q}$ are radical over $\mathbb{Q}$.*

Proof. Let $\alpha = \omega\sqrt[4]{3}$, where ω is a primitive cube root of unity, and let $R = \mathbb{Q}[\alpha]$. Since α^{12} is rational, R is radical, and $|R : \mathbb{Q}| \leq 12$. Observe that $\omega = \alpha^4/3 \in R$, and thus $i\sqrt{3} \in R$. Also, $\sqrt[4]{3} = \alpha/\omega \in R$, and thus $\sqrt{3} \in R$, and we see that $i \in R$. Thus R contains the splitting field F of $X^4 - 3$ over $\mathbb{Q}$. Since $8 = |F : \mathbb{Q}|$ divides $|R : \mathbb{Q}|$ and $|R : \mathbb{Q}| \leq 12$, we deduce that $F = R$, and so F is radical over $\mathbb{Q}$, as claimed.

To handle the polynomial $X^4 + 3$, we do a similar computation, but now we let $\alpha = \omega\sqrt{2}\sqrt[4]{3}$. Here, too, α^{12} is rational, and so $R = \mathbb{Q}[\alpha]$ is radical and $|R : \mathbb{Q}| \leq 12$. Also, $\omega = \alpha^4/12 \in R$, and thus as in the previous case, $i\sqrt{3} \in R$. Furthermore, $\sqrt{2}\sqrt[4]{3} = \alpha/\omega \in R$, and it follows that $\sqrt{3} \in R$, and thus in this case, too, $i \in R$. Now let $\beta = (1+i)\sqrt{2}\sqrt[4]{3}/2$, so that $\beta \in R$ and $\beta^4 = -3$. It follows that R contains (and hence must be) the splitting field of $X^4 + 3$ over $\mathbb{Q}$. □

In view of the previous result, it seems natural to try to determine all square-free integers k with $|k| > 1$ and such that the splitting field of $X^4 - k$ is radical over $\mathbb{Q}$. We show that this happens only for $k = \pm 3$. We shall see that Corollary B suffices to eliminate all cases where $|k| > 3$, but the situation when $|k| = 2$ is more subtle.

Theorem 3.4. *Let k be a square-free integer with $|k| > 1$ and such that the splitting field of $X^4 - k$ over $\mathbb{Q}$ is radical over $\mathbb{Q}$. Then $k = \pm 3$.*

Proof. Let E be the splitting field of $X^4 - k$ over $\mathbb{Q}$. Since $X^4 - k$ is irreducible, $|E : \mathbb{Q}|$ is a multiple of 4, and since $E = \mathbb{Q}[\beta, i]$, where $\beta^4 = k$, it follows that $|E : \mathbb{Q}|$ is 4 or 8. But if $|E : \mathbb{Q}| = 4$, then since $\beta^4 \in \mathbb{Q}$ and $\mathrm{Gal}(E/\mathbb{Q})$ is abelian, we can apply Lemma 2.3 to deduce that $|\beta|^2$ is rational. But $|\beta|^2 = \sqrt{|k|}$, which is irrational, and this is a contradiction. We conclude that $|E : \mathbb{Q}| = 8$, and thus $\mathrm{Gal}(E/\mathbb{Q})$, which we know can be embedded in the symmetric group S_4, must be isomorphic to the dihedral group D_8. In particular, E is not a cyclotomic field, and so $m > 1$, and thus since m divides $|E : \mathbb{Q}| = 8$, we must have $m = 2$ by Corollary B. It follows that $|K : \mathbb{Q}| = 4$, where K is the maximum cyclotomic subfield of E. Thus $\mathrm{Gal}(K/\mathbb{Q})$ is a homomorphic image of D_8 of order 4, and this forces $K = \mathbb{Q}_8$ or $K = \mathbb{Q}_{12}$, and hence either $\sqrt{2} \in E$ or $\sqrt{3} \in E$. Since D_8 has exactly three maximal subgroups, there are just three quadratic subfields in E. These are $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{|k|}]$ and $\mathbb{Q}[i\sqrt{|k|}]$, and of these, only $\mathbb{Q}[\sqrt{|k|}]$ is real. Thus $\mathbb{Q}[\sqrt{|k|}]$ must be either $\mathbb{Q}[\sqrt{2}]$ or $\mathbb{Q}[\sqrt{3}]$, and since k is square-free, it is easy to see that $|k|$ must be 2 or 3.

It now suffices to show that the splitting fields of $X^4 - 2$ and $X^4 + 2$ are not radical over $\mathbb{Q}$. In fact, these polynomials have the same splitting field E, and so there is really only one case to consider. (To see that these splitting fields are the same, observe that each of them contains $(1 + i)/\sqrt{2}$, which is a primitive 8th root of unity.)

Observe that $\mathbb{Q}_8 = \mathbb{Q}[i, \sqrt{2}] \subseteq E$ and $|E : \mathbb{Q}_8| = 2$. Also, E is not cyclotomic since $\mathrm{Gal}(E/\mathbb{Q})$ is nonabelian, and thus $\mathbb{Q}_8$ is the maximum cyclotomic field in E, and hence $K = \mathbb{Q}_8$ and $m = 2$ in our usual notation. Working by contradiction, assume that E is radical over $\mathbb{Q}$, and write $E = \mathbb{Q}[\alpha]$, where $\alpha^n \in \mathbb{Q}$ for some positive integer n, which we assume to be minimal. Then $\mathbb{Q}_n \subseteq E$ by Lemma 2.1, and hence $\mathbb{Q}_n \subseteq K = \mathbb{Q}_8$. But $n \geq |E : \mathbb{Q}| = 8$, and we conclude that $n = 8$. Also, since we can replace α by a rational multiple if necessary, we can assume that $\alpha^8 \in \mathbb{Z}$.

Now $\alpha^2 \in K$ by Lemma 2.2, and thus $\alpha^2 = \delta\sqrt{r}$ by Lemma 2.3, where δ is an 8th root of unity and r is a positive rational number. Furthermore, since α^4 is not rational, δ^2 is also not rational, and hence δ is a primitive 8th root of unity. We can thus write $\alpha = \epsilon\sqrt[4]{r}$, where ϵ is a primitive 16th root of unity. Also, $-r^2 = \alpha^8 \in \mathbb{Z}$, and since r is rational, $r \in \mathbb{Z}$. Write $r = uv$, where u is the 2-part of r and v is the odd part.

Let $L = \langle E, \mathbb{Q}_{16} \rangle$, so that $\alpha \in L$ and $\epsilon \in L$, and thus $\sqrt[4]{r} \in L$. Since $\sqrt[4]{2} \in E$, we have $\sqrt[4]{u} \in E \subseteq L$, and thus $\sqrt[4]{v} \in L$.

Now L is Galois over $\mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q})$ has order 16. Also, $\mathrm{Gal}(E/\mathbb{Q})$ is a nonabelian homomorphic image of G, so G is nonabelian. But $\mathrm{Gal}(\mathbb{Q}_{16}/\mathbb{Q})$ is an abelian homomorphic image of G of order 8, and hence it is the full commutator factor group of $\mathrm{Gal}(L/\mathbb{Q})$. Since $\mathrm{Gal}(\mathbb{Q}_{16}/\mathbb{Q})$ has exactly three subgroups of index 2, it follows that G also has exactly three such subgroups, and so L contains exactly three quadratic extensions of $\mathbb{Q}$. These are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i]$ and $\mathbb{Q}[i\sqrt{2}]$, and thus L does not contain $\sqrt{k}$ for any nonsquare odd integer k. Since $\sqrt[4]{v} \in L$, and v is odd, we conclude that $\sqrt[4]{v} \in \mathbb{Q}$.

Since $\sqrt[4]{u} \in E$ and $\sqrt[4]{v} \in \mathbb{Q}$, we have $\sqrt[4]{r} \in E$. But $\alpha = \epsilon\sqrt[4]{r}$ and $\alpha \in E$, and thus $\epsilon \in E$. This is a contradiction, however, because ϵ is a primitive 16th root of unity. □

We mention that the part of the preceding proof where we showed that $\sqrt[4]{v}$ is rational (in the second and third paragraphs from the end) can be replaced by an argument involving ramification of rational primes. First, it is not hard to compute that the discriminant of the extension $\mathbb{Q} \subseteq E$ is plus or minus a power of 2, and thus 2 is the only rational prime that can ramify in this extension. On the other hand, if we write $\alpha^8 = a$ and assume (as we may) that a is an 8th-power-free integer, then every prime divisor of a must ramify, and thus a is plus or minus a power of 2. The integer v appearing in the above proof, therefore, is actually 1.

References

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* 2nd ed., Clarendon, Oxford, 1945. MR0067125 (16:673c)

[2] I. M. Isaacs, *Algebra: a graduate course,* Brooks/Cole, Pacific Grove, 1994. MR1276273 (95k:00003)

Department of Mathematics, Wayne State University, 656 W. Kirby, Detroit, Michigan 48202

E-mail address: dgluck@math.wayne.edu

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

E-mail address: isaacs@math.wisc.edu