Canad. Math. Bull. Vol. 64 (4), 2021, pp. 877–885
http://dx.doi.org/10.4153/S0008439520000909

On the degree of repeated radical extensions

Fernando Szechtman

Abstract. We answer a question posed by Mordell in 1953, in the case of repeated radical extensions, and find necessary and sufficient conditions for $[F[\sqrt[m_1]{N_1},\dots,\sqrt[m_\ell]{N_\ell}]:F]=m_1\cdots m_\ell$, where F is an arbitrary field of characteristic not dividing any m_i.

1 Introduction

We fix throughout a unique factorization domain D with field of fractions F, allowing for the possibility that $D=F$, and write $c(F)$ for the characteristic of F. We also fix $\ell\in\mathbb{N}$, $m_1,\dots,m_\ell\in\mathbb{N}$, $m=\operatorname{lcm}\{m_1,\dots,m_\ell\}$, and $N_1,\dots,N_\ell\in D$. A *prime* means a prime positive integer.

In this paper, we give a necessary and sufficient condition for

$$\left[F[\sqrt[m_1]{N_1},\dots,\sqrt[m_\ell]{N_\ell}]:F\right]=m_1\cdots m_\ell, \tag{1.1}$$

assuming only $c(F)\nmid m$. This settles a problem posed by Mordell [M] in 1953, in the case of repeated radical extensions.

The degrees of repeated radical extensions have been studied by several authors, including Hasse [H], Besicovitch [B], Mordell [M], Siegel [S], Richards [Ri], Ursell [U], Zhou [Z], Albu [A], and Carr and O'Sullivan [CO].

The question of when $[F[\sqrt[n]{a}]:F]=n$ was solved by Vahlen [V] in 1895 if $F=\mathbb{Q}$, Capelli [C] in 1897 if F has characteristic 0, and Rédei [R, Theorem 428] in 1959 in general.

Irreducibility Criterion (C). The polynomial $X^n-a\in F[X]$ is irreducible if and only if $a\notin F^p$ for every prime factor p of n, and if $4|n$, then $a\notin -4F^4$.

In particular, if $-a\notin F^2$ and $a\notin F^p$ for every prime factor p of n, then X^n-a is irreducible. The special case of (C) when n is prime is due to Abel; a very simple proof of this case can be found in [R, Theorem 427].

Provided F contains a primitive m-th root of unity, Hasse [H] showed that (1.1) holds if and only if

$$(\sqrt[m_1]{N_1})^{a_1}\times\cdots\times(\sqrt[m_\ell]{N_\ell})^{a_\ell}\in F,\ a_i\geq 0,\ \text{ only when } m_1|a_1,\dots,m_\ell|a_\ell. \tag{1.2}$$

Received by the editors July 20, 2020; revised November 14, 2020.
Published online on Cambridge Core November 23, 2020.
This paper is dedicated to Natalio H. Guersenzvaig. This research was partially supported by an NSERC grant.
AMS subject classification: **12F05, 12F10, 12E05.**
Keywords: Radical extension, Galois extension, Vahlen-Capelli irreducibility criterion.

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press

Later, Besicovitch [B] proved (1.1) assuming: $D = \mathbb{Z}$; each N_i is positive and has a prime factor that divides it only once and does not divide any other N_j; each $\sqrt[m_i]{N_i}$ is positive and real (the $m_1 \cdots m_\ell$ embeddings of $\mathbb{Q}[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}]$ into $\mathbb{C}$ then yield (1.1) for all other m_i-th roots of the N_i). The special case of Besicovitch's result when $m_1 = \cdots = m_\ell$ and every N_i is prime appears in Richards [Ri] (for the more elementary case $m_1 = \cdots = m_\ell = 2$, see [F, Ro]). Assuming that $N_1, \dots, N_\ell$ are pairwise relatively prime, Ursell [U] obtained a variation of Besicovitch's theorem.

Mordell [M] combined and extended the results of Hasse and Besicovitch, and proved (1.1) assuming (1.2), and that F contains a primitive m-th root of unity or that F is a subfield of $\mathbb{R}$ with all $\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}$ real. In the latter case, all N_i such that m_i is even must be positive. Siegel [S] gave a theoretical description of the value of $[F[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}] : F]$ under Mordell's condition that F be a subfield of $\mathbb{R}$ with all $\sqrt[m_i]{N_i}$ real. Albu [A] extended the work of Mordell and Siegel to the case when F contains a primitive m-th root of unity or all m-th roots of unity in $F[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}]$ belong to $\{1, -1\}$. Under these weaker assumptions, (1.1) is still shown in [A] to be a consequence of (1.2). It is worth noting that, except for (1.2), none of the aforementioned conditions are necessary for (1.1) to hold. A different approach was taken by Zhou [Z], using valuation theory, when F is an algebraic number field; he succeeded in avoiding any assumptions on roots of unity and proved a more general version of (1.1), applicable to repeated extensions via Eisenstein polynomials, not just binomials. Nevertheless, Zhou's hypotheses are also unnecessary for (1.1) to hold. Indeed, when the ring of integers of F is a UFD, each N_i is forced to have an irreducible factor that divides it only once and does not divide any other N_j. More recently, Carr and O'Sullivan [CO] proved a fairly general result on the linear independence of roots and reproved Mordell's theorem as an application.

Set $J = \{1, \dots, \ell\}$, $\mathcal{P} = \{p \mid p \text{ is a prime factor of } m\}$, and for each $i \in J$ and $p \in \mathcal{P}$, let $m_i(p)$ be the p-part of m_i, so that $m_i(p) = p^{n_i}$, where $n_i \geq 0$, $p^{n_i} | m_i$ and $p^{n_i+1} \nmid m_i$. It is clear that

$$\Big[F[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}] : F\Big] = m_1 \cdots m_\ell \iff \tag{1.3}$$
$$\Big[F[\sqrt[m_1(p)]{N_1}, \dots, \sqrt[m_\ell(p)]{N_\ell}] : F\Big] = m_1(p) \cdots m_\ell(p)$$

for all $p \in \mathcal{P}$. We are thus reduced to study the case when each $m_i = m_i(p)$ for a fixed prime p. We split this case in two subcases depending on the parity of p. For each prime p, we set

$$\mathcal{S}_p = \Big\{N_1, N_1^{e_1} N_2, N_1^{e_1} N_2^{e_2} N_3, \dots, N_1^{e_1} \cdots N_{\ell-1}^{e_{\ell-1}} N_\ell, 0 \leq e_i < p\Big\}.$$

In particular, $\mathcal{S}_2$ consists of all $N_1^{e_1} \cdots N_\ell^{e_\ell}$ such that $e_i \in \{0, 1\}$ and $(e_1, \dots, e_\ell) \neq (0, \dots, 0)$.

Theorem 1.1 *Let $n_1, \dots, n_\ell \in \mathbb{N}$, p an odd prime such that $c(F) \neq p$, and suppose $m_i = p^{n_i}$ for all $i \in J$. Then (1.1) holds if and only if $\mathcal{S}_p \cap D^p = \emptyset$.*

The well-known example $[\mathbb{Q}[\sqrt[4]{-1}, \sqrt[4]{2}] : \mathbb{Q}] = 8$ shows that Theorem 1.1 fails if $p = 2$. The above criteria impose general conditions that disallow this example. Close examination of numerous pathological cases led us to the exact conditions required

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press

when $p = 2$. We say that $(N_1, \dots, N_\ell)$ is 2-defective if the following two conditions hold: $\mathcal{S}_2 \cap D^2 = \emptyset$ but $\mathcal{S}_2 \cap (-D^2) \neq \emptyset$ (this readily implies that $|\mathcal{S}_2 \cap (-D^2)| = 1$, as shown in Lemma 2.5); if $-d^2 = M = N_1^{f_1} \cdots N_\ell^{f_\ell}$ is the only element of $\mathcal{S}_2 \cap (-D^2)$, where $d \in D$, $0 \leq f_i < 2$, and $M^\sharp = \{i \in J \mid f_i = 1\}$ is nonempty (since $\mathcal{S}_2 \cap D^2 = \emptyset$, the exponents f_i are uniquely determined by M, whence $M^\sharp$ is well defined), then $4 | m_i$ for all $i \in M^\sharp$, and if $i \in M^\sharp$, then

$$\pm 2d \prod_{j \neq i} N_j^{e_j} \in D^2 \text{ for some choice of } 0 \leq e_j < 1. \tag{1.4}$$

Since $-M = N_1^{f_1} \cdots N_\ell^{f_\ell} \in D^2$, the outcome of (1.4) is independent of the actual choice of $i \in M^\sharp$.

Theorem 1.2 *Let $n_1, \dots, n_\ell \in \mathbb{N}$ and suppose that $c(F) \neq 2$ and $m_i = 2^{n_i}$ for all $i \in J$. Then (1.1) holds if and only if $\mathcal{S}_2 \cap D^2 = \emptyset$ and $(N_1, \dots, N_\ell)$ is not 2-defective.*

Combining (1.3) with Theorems 1.1 and 1.2, we immediately obtain a general criterion for (1.1). This requires additional notation. For each $p \in \mathcal{P}$, we set $J(p) = \{i \mid i \in J \text{ and } p | m_i\}$, and write

$$\begin{aligned} J(p) &= \{i(p,1), \dots, i(p, \ell(p))\}, \quad i(p,1) < \cdots < i(p, \ell(p)), \\ \mathcal{S}(p) &= \{N_{i(p,1)}, N_{i(p,1)}^{e_1} N_{i(p,2)}, N_{i(p,1)}^{e_1} N_{i(p,2)}^{e_2} N_{i(p,3)}, \dots, N_{i(p,1)}^{e_1} \\ &\qquad \cdots N_{i(p,\ell(p)-1)}^{e_{\ell(p)-1}} N_{i(p,\ell(p))}, 0 \leq e_j < p\}. \end{aligned}$$

Theorem 1.3 *Suppose that $c(F) \neq m$. Then (1.1) holds if and only if $\mathcal{S}(p) \cap D^p = \emptyset$ for every $p \in \mathcal{P}$ and, if $2 \in \mathcal{P}$, then $(N_{i(2,1)}, \dots, N_{i(2,\ell(2))})$ is not 2-defective.*

The next example illustrates the use of Theorems 1.2 and 1.3, and lies outside of the scope of the aforementioned criteria.

Example 1.4 Suppose that $-1 \notin F^2$ and each of $A, B, C \in D$ has an irreducible factor that divides it only once and does not divide any of the two other elements. Then

$$[F[\sqrt[m_1]{AB}, \sqrt[m_2]{BC}, \sqrt[m_3]{-CA}] : F] = m_1 m_2 m_3$$

if and only if at least one of m_1, m_2, m_3 is not divisible by 4 or none of $\pm 2A, \pm 2B, \pm 2C \in D^2$.

As we are dealing with a classical and basic problem, we purposely resort to elementary and complete arguments in order to maximize the potential readership of our solution.

2 Lemmata

Given a nonzero $a \in F$, we write $\langle a \rangle$ for the subgroup of $F^\times$ generated by a.

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press

Lemma 2.1 *Let p be a prime such that $c(F)\neq p$ and suppose $b_1,\dots,b_n\in F$ are nonzero. Then*

$$F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_n}]^p\cap F=F^p\langle b_1,\dots,b_n\rangle. \tag{2.1}$$

Proof Let $M,N\in F$ be nonzero. We claim that if $\sqrt[p]{M}\in F[\sqrt[p]{N}]$, then $M\in F^p\langle N\rangle$. This is clear if $N\in F^p$, so we assume $N\notin F^p$.

Set $K=F[\zeta]$, where ζ is a primitive p-th root of unity. Then K/F is a Galois extension with Galois group isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular, $[K:F]$ divides $p-1$. It follows that $K^p\cap F=F^p$. Indeed, suppose $a\in F$ and $\alpha\in K$ satisfies $\alpha^p=a$. Since $[F[\alpha]:F]$ divides $[K:F]$, it also divides $p-1$. As $p\nmid(p-1)$, $X^p-a\in F[X]$ is reducible, whence $a\in F^p$ by (C).

By assumption, $N\notin F^p$. Thus, $N\notin K^p$ as indicated above, so $X^p-N\in K[X]$ is irreducible by (C). Thus $\{1,\sqrt[p]{N},\dots,\sqrt[p]{N^{p-1}}\}$ is a K-basis of $K[\sqrt[p]{N}]$. By assumption, $\sqrt[p]{M}\in K[\sqrt[p]{N}]$, so

$$\sqrt[p]{M}=a_0+a_1\sqrt[p]{N}+\cdots+a_{p-1}\sqrt[p]{N^{p-1}},\quad a_i\in K. \tag{2.2}$$

Note that $K[\sqrt[p]{N}]/K$ is a Galois extension with cyclic Galois group $\langle\sigma\rangle$, where $\sigma(\sqrt[p]{N})=\zeta\sqrt[p]{N}$. Since $\sqrt[p]{M}$ is a root of X^p-M, we must have $\sigma(\sqrt[p]{M})=\zeta^i\sqrt[p]{M}$ for some $0\leq i<p$. Applying σ to (2.2), we obtain

$$\zeta^i\sqrt[p]{M}=a_0+a_1\zeta\sqrt[p]{N}+\cdots+a_{p-1}\zeta^{p-1}\sqrt[p]{N^{p-1}}.$$

On the other hand, multiplying (2.2) by ζ^i yields

$$\zeta^i\sqrt[p]{M}=a_0\zeta^i+a_1\zeta^i\sqrt[p]{N}+\cdots+a_{p-1}\zeta^i\sqrt[p]{N^{p-1}}.$$

From the K-linear independence of $1,\sqrt[p]{N},\dots,\sqrt[p]{N^{p-1}}$ we infer that $a_j=0$ for all $j\neq i$. Thus

$$\sqrt[p]{M}=a\sqrt[p]{N^i},\quad a\in K,$$

whence $M=a^pN^i$. Thus $M/N^{-i}\in K^p\cap F=F^p$, so $M\in F^p\langle N\rangle$.

By above, $F[\sqrt[p]{b_1}]^p\cap F=F^p\langle b_1\rangle$. Suppose $n>1$ and $F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}]^p\cap F=F^p\langle b_1,\dots,b_{n-1}\rangle$. Then

$$\begin{aligned}&F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}},\sqrt[p]{b_n}]^p\cap F\\&\quad=(F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}][\sqrt[p]{b_n}])^p\cap F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}]\cap F\\&\quad=F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}]^p\langle b_n\rangle\cap F.\end{aligned}$$

Let $\alpha\in F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}]^p\langle b_n\rangle\cap F$. Then $\alpha\in F$ and $\alpha b_n^i\in F[\sqrt[p]{b_1},\dots,\sqrt[p]{b_{n-1}}]^p\cap F$ for some $i\in\mathbb{Z}$. Thus $\alpha b_n^i\in F^p\langle b_1,\dots,b_{n-1}\rangle$ and so $\alpha\in F^p\langle b_1,\dots,b_{n-1},b_n\rangle$. ■

Lemma 2.2 *Suppose $-1\notin F^2$ and $\pm a\notin F^2$. Then for any $n\in\mathbb{N}$, we have that $\sqrt{-1}\notin F[\sqrt[2^n]{a}]$.*

Proof We show by induction that $\sqrt{-1} \notin F[\sqrt[2^n]{a}]$ and $\pm\sqrt[2^n]{a} \notin F[\sqrt[2^n]{a}]^2$. The fact that $\sqrt{-1} \notin F[\sqrt{a}]$ follows from Lemma 2.1. Suppose, if possible, that $\pm\sqrt{a} = z^2$, where $z \in F[\sqrt{a}]$. Then $z = x + y\sqrt{a}$, where $x, y \in F$, so that $\pm\sqrt{a} = x^2 + ay^2 + 2xy\sqrt{a}$. It follows that $x^2 + ay^2 = 0$. As $-a \notin F^2$, we infer $x = y = 0$, a contradiction.

Assume we have shown that $\sqrt{-1} \notin F[\sqrt[2^n]{a}]$ and $\pm\sqrt[2^n]{a} \notin F[\sqrt[2^n]{a}]^2$ for some $n \in \mathbb{N}$. Since $\pm a \notin F^2$, (C) implies $[F[\sqrt[2^n]{a}] : F] = 2^n$ and $[F[\sqrt[2^{n+1}]{a}] : F] = 2^{n+1}$. But $\sqrt{-1} \notin F[\sqrt[2^n]{a}]$, so $F[\sqrt[2^{n+1}]{a}] = F[\sqrt[2^n]{a}, \sqrt{-1}]$. Thus $\sqrt[2^{n+1}]{a} = \alpha + \beta\sqrt{-1}$ for unique $\alpha, \beta \in F[\sqrt[2^n]{a}]$. Squaring, we get $\sqrt[2^n]{a} = \alpha^2 - \beta^2 + 2\alpha\beta\sqrt{-1}$, which implies $\alpha\beta = 0$ and $\alpha^2 - \beta^2 = \sqrt[2^n]{a}$, a contradiction. ■

Lemma 2.3 *Suppose $c(F) \neq 2$, let $n \in \mathbb{N}$, and set $K = F[\zeta]$, where ζ is a primitive 2^n-th root of unity. If $n \leq 2$ or $-1 \in F^2$, then $G = \mathrm{Gal}(K/F)$ is cyclic.*

Proof We have an embedding $\Psi : G \to (\mathbb{Z}/2^n\mathbb{Z})^\times$, $\sigma \to [s]$, where $\sigma(\zeta) = \zeta^s$. This settles the case $n \leq 2$. Assume henceforth that $n \geq 3$. We have $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle a, b \rangle$, where $a = [5]$, $b = [-1]$ and $\langle a \rangle \cap \langle b \rangle$ is trivial [Vi, Chapter VI]. By hypothesis, $-1 = \alpha^2$, where $\alpha \in F \cap \langle \zeta \rangle$. Suppose, if possible, that $b \in \Psi(G)$, say $b = \Psi(\sigma)$. Then $\sigma(\alpha) = \alpha^{-1} = -\alpha$, since α is a power of ζ, and $\sigma(\alpha) = \alpha$, since $\alpha \in F$. This contradiction shows that $b \notin \Psi(G)$. Now any subgroup S of $\langle a, b \rangle$ that does not contain b must be cyclic (if S is not trivial, it is generated by a^i or $a^i b$, where i is the smallest positive integer such that an element of this type is in S). Thus G is cyclic. ■

Lemma 2.4 *Let $n \in \mathbb{N}$, p an odd prime such that $c(F) \neq p$, and set $K = F[\zeta]$, where ζ is a primitive p^n-th root of unity. Then $\mathrm{Gal}(K/F)$ is cyclic.*

Proof $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, which is a cyclic group. ■

Lemma 2.5 *Suppose $\mathcal{S}_2 \cap D^2 = \emptyset$. Then $|\mathcal{S}_2 \cap (-D^2)| \leq 1$, with $|\mathcal{S}_2 \cap (-D^2)| = 0$ if $-1 \in F^2$.*

Proof Suppose $M \neq N$ are in $\mathcal{S}_2 \cap (-D^2)$. Then $MN \in D^2$ and $MN = e^2P$, where $P \in \mathcal{S}_2$ and $e \in D$. Thus, $P \in D^2$, against $\mathcal{S}_2 \cap D^2 = \emptyset$. If $-1 \in F^2$, then $-D^2 = D^2$, so $\mathcal{S}_2 \cap (-D^2) = \emptyset$. ■

Lemma 2.6 *Suppose $c(F) \neq 2$, let $n \in \mathbb{N}$ and set $K = F[\zeta]$, where ζ is a primitive 2^nth root of unity. Assume that $\mathcal{S}_2 \cap D^2 = \emptyset$. Then $|\mathcal{S}_2 \cap K^2| \in \{0, 1, 3\}$. Moreover, if $|\mathcal{S}_2 \cap K^2| = 3$ then one of the elements of $\mathcal{S}_2 \cap K^2$ is in $\mathcal{S}_2 \cap (-D^2)$, and we have $-1 \notin F^2$, $n \geq 3$.*

Proof Suppose $M \neq N$ are in $\mathcal{S}_2 \cap K^2$. Then $MN \in K^2$ and $MN = e^2P$, where $P \in \mathcal{S}_2$ and $e \in D$, so $P \in D^2$. Lemma 2.1 implies that $F[\sqrt{M}], F[\sqrt{N}], F[\sqrt{P}]$ are distinct intermediate subfields of K/F of degree 2. In particular, $\mathrm{Gal}(K/F)$ is not cyclic. Now $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/2^n\mathbb{Z})^\times$, so $n \geq 3$ and $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong (\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Any subgroup of $(\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has at most 3 subgroups of index 2, so the Galois correspondence implies that any intermediate subfield of

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press

K/F of degree 2 must be equal to one of $F[\sqrt{M}], F[\sqrt{N}], F[\sqrt{P}]$. Lemma 2.1 readily implies that no element from $\mathcal{S}_2$ different from M, N, P is in K^2. By Lemma 2.3, $-1 \notin F^2$, so $F[\sqrt{-1}]$ must be equal to one of $F[\sqrt{M}], F[\sqrt{N}], F[\sqrt{P}]$, and Lemma 2.1 implies that one of M, N, P is in $-D^2$. ■

Lemma 2.7 *Let $n_1, \dots, n_\ell \in \mathbb{N}$ and p a prime such that $c(F) \neq p$ and $m_i = p^{n_i}$ for all $i \in J$. Let $K = F[\zeta]$, where ζ is a primitive m-th root of unity, $m = \operatorname{lcm}\{m_1, \dots, m_\ell\}$. Suppose that $\mathcal{S}_p \cap K^p = \emptyset$. Then $[K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}] : K] = m_1 \cdots m_\ell$.*

Proof By assumption $N_1 \notin K^p$. Moreover, if $4|m_1$, then $-1 \in K^2$ and therefore $-N_1 \notin K^2$. It follows from (C) that we have $[K[\sqrt[m_1]{N_1}] : K] = m_1$. Suppose $[K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}] : K] = m_1 \cdots m_i$ for some $1 \leq i < \ell$.

Assume, if possible, that $\sqrt[p]{N_{i+1}} \in K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}]$. Then $K[\sqrt[p]{N_{i+1}}]$ is an intermediate subfield of degree p in the Galois extension $K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}]/K$, with Galois group $G = \langle \sigma_1, \dots, \sigma_i \rangle$, where

$$\sigma_k(\sqrt[m_k]{N_k}) = \zeta^{m/m_k} \sqrt[m_k]{N_k}, \ \sigma_k(\sqrt[m_j]{N_j}) = \sqrt[m_j]{N_j}, \ j \neq k.$$

Any subgroup of G of index p contains G^p, so by the Galois correspondence $K[\sqrt[p]{N_{i+1}}]$ is contained in the fixed field of G^p, namely $K[\sqrt[p]{N_1}, \dots, \sqrt[p]{N_i}]$. Lemma 2.1 implies that $N_1^{e_1} \cdots N_i^{e_i} N_{i+1} \in K^p$ for some $0 \leq e_i < p$, against $\mathcal{S}_p \cap K^p = \emptyset$. Thus $\sqrt[p]{N_{i+1}} \notin K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}]$.

Assume if possible, that $4|m_{i+1}$ and $\sqrt{-N_{i+1}} \in K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}]$. Then the above argument yields $N_1^{e_1} \cdots N_i^{e_{i+1}} N_{i+1} \in -K^2$ for some $0 \leq i < p$. But $-K^2 = K^2$, so $\mathcal{S}_p \cap K^p = \emptyset$ is violated. This shows $\sqrt{-N_{i+1}} \notin K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_i]{N_i}]$ when $4|m_{i+1}$.

We deduce from (C) that $[K[\sqrt[m_1]{N_1}, \dots, \sqrt[m_{i+1}]{N_{i+1}}] : K] = m_1 \cdots m_{i+1}$. ■

Lemma 2.8 *Let $n_1, \dots, n_\ell \in \mathbb{N}$ and p a prime such that $c(F) \neq p$ and $m_i = p^{n_i}$ for all $i \in J$. Let $K = F[\zeta]$, where ζ is a primitive mth root of unity, $m = \operatorname{lcm}\{m_1, \dots, m_\ell\}$. Suppose that $\mathcal{S}_p \cap D^p = \emptyset$ and $|\mathcal{S}_p \cap K^p| = 1$, say $M = N_1^{f_1} \cdots N_\ell^{f_\ell}$, where $0 \leq f_i < p$, and $M^\sharp = \{i \in J \mid f_i = 1\}$ is nonempty. For $i \in M^\sharp$, set $V_i = \{\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}\} \setminus \{\sqrt[m_i]{N_i}\}$ and let $m[i]$ be the product of all m_j with $j \neq i$. Then*

(i) *$[K[V_i] : K] = m[i]$ and $\sqrt[p]{N_i} \notin F[V_i]$ for all $i \in M^\sharp$.*
(ii) *If p is odd or $m_i = 2$ for at least one $i \in M^\sharp$, then (1.1) holds.*
(iii) *If $4|m$ and $\mathcal{S}_2 \cap (-D^2) = \emptyset$, then $\sqrt{-N_i} \notin F[V_i]$ for all $i \in M^\sharp$, so (1.1) holds.*
(iv) *If $4|m_i$ for all $i \in M^\sharp$ and $M \in \mathcal{S}_2 \cap (-D^2)$, say $M = -d^2$ with $d \in D$, then (1.1) holds if and only if given any $i \in M^\sharp$, (1.4) fails.*

Proof Let $i \in M^\sharp$. By Lemma 2.7, $[K[V_i] : K] = m[i]$ and hence $[F[V_i] : F] = m[i]$. Suppose, if possible, that $\sqrt[p]{N_i} \in F[V_i]$ and set $Y_i = \{\zeta\} \cup V_i$. Then $F[\sqrt[p]{N_i}]$ is an intermediate subfield of degree p in the Galois extension $F[Y_i]/F$, with Galois group $G = H \rtimes U$, where $H = \langle \sigma_j \mid j \neq i \rangle$ is the Galois group of $F[Y_i]/F[\zeta]$ and each σ_k is as in the proof of Lemma 2.7, and U is the Galois group of $F[Y_i]/F[V_i]$. The subgroup S of G corresponding to $F[\sqrt[p]{N_i}] \subseteq F[V_i]$ in the Galois correspondence has index p and contains U. Therefore, $S \supseteq H^p \rtimes U$, so $F[\sqrt[p]{N_i}]$ is contained in the fixed field of $H^p \rtimes U$, namely $F[W_i]$, where $W_i = \{\sqrt[p]{N_1}, \dots, \sqrt[p]{N_\ell}\} \setminus \{\sqrt[p]{N_i}\}$. It

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press

follows from Lemma 2.1 that $N_1^{e_1} \cdots N_\ell^{e_\ell} \in F^p$, where all $0 \le e_j < p$ and $e_i = 1$. By the rational root theorem, $F^p \cap D = D^p$, so $\mathcal{S}_p \cap D^p = \emptyset$ is violated.

If $m_i = 2$ for at least one $i \in M^\sharp$, then (1.1) has been established. Likewise, if p is odd, then (1.1) follows from (C). Suppose next that $4|m$ and $\mathcal{S}_2 \cap (-D^2) = \emptyset$. We claim that $\sqrt{-N_i} \notin F[V_i]$. If not, arguing as above, we see that $-N_1^{e_1} \cdots N_\ell^{e_\ell} \in F^2 \subseteq K^2$, where all $0 \le e_j < 2$ and $e_i = 1$. On the other hand, $M \in K^2$ and $-1 \in K^2$, so $-M \in K^2$ and therefore the product of all $N_j^{e_j + f_j}$, with $j \neq i$, must be in K^2. The uniqueness of M in $\mathcal{S}_2 \cap K^2$ forces $e_j = f_j$ for all $j \neq i$. Thus $-M \in F^2$ and hence $M \in \mathcal{S}_2 \cap (-D^2)$, a contradiction. Thus (1.1) follows from (C) in this case as well.

Suppose finally that $4|m_i$ for all $i \in M^\sharp$ and $M \in \mathcal{S}_2 \cap (-D^2)$, say $M = -d^2$ with $d \in D$. Fix any $i \in M^\sharp$ and set $L_i = F[V_i]$. It remains to decide when $N_i \in -4L_i^4$. Since $4|m_j$ for all $j \in M^\sharp$, the product of all $N_j^{f_j}$ with $j \neq i$ and $j \in M^\sharp$, belongs to L_i^4. Thus,

$$N_i \in -4L_i^4 \Leftrightarrow M \in -4L_i^4 \Leftrightarrow d^2 \in 4L_i^4 \Leftrightarrow \pm 2d \in L_i^2,$$

and, by Lemma 2.1, this happens if and only if (1.4) holds. ∎

3 Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1 It is clear that (1.1) implies $\mathcal{S}_p \cap D^p = \emptyset$. Suppose $\mathcal{S}_p \cap D^p = \emptyset$ and let $K = F[\zeta]$, where ζ is a primitive m-th root of unity. By Lemmas 2.7 and 2.8, it suffices to show that $|\mathcal{S}_p \cap K^p| \le 1$. Suppose not and let $M \neq N$ be in $\mathcal{S}_p \cap K^p$. As M, N have degree p over F, we see that $p|[K : F]$. By Lemma 2.4, $\mathrm{Gal}(K/F)$ has a unique subgroup of index p, so by the Galois correspondence, K/F has a unique intermediate field of degree p. We deduce $F[\sqrt[p]{M}] = F[\sqrt[p]{N}]$, and Lemma 2.1 implies $MN^i \in F^p$ for some $i \in \mathbb{Z}$. Since $M \neq N$, this is disallowed by $\mathcal{S}_p \cap D^p = \emptyset$. ∎

Proof of Theorem 1.2 It is clear that $\mathcal{S}_2 \cap D^2 = \emptyset$ follows from (1.1). Suppose that $\mathcal{S}_2 \cap D^2 = \emptyset$. We will show that (1.1) holds if and only if $(N_1, \dots, N_\ell)$ is not 2-defective.

By Lemmas 2.6, 2.7, and 2.8, we can restrict to the case when $|\mathcal{S}_2 \cap K| = 3$, in which case, by Lemmas 2.5 and 2.6, there is a single element $M \in \mathcal{S}_2 \cap (-D^2)$, and we necessarily have $-1 \notin F^2$ and $8|m$.

Now $-d^2 = M = N_1^{f_1} \cdots N_\ell^{f_\ell}$, where $0 \le f_i < 2$ and $M^\sharp = \{i \in J \mid f_i = 1\}$ is nonempty. Fix any $i \in M^\sharp$ and let S_2^i stand for the analogue of S_2 corresponding to $\{N_1, \dots, N_\ell\} \setminus \{N_i\}$. By the uniqueness of M in $\mathcal{S}_2 \cap (-D^2)$, we see that $\mathcal{S}_2^i \cap (-D^2) = \emptyset$. It follows from Lemma 2.6 that $|\mathcal{S}_2^i \cap K^2| \le 1$.

Suppose first that $|\mathcal{S}_2^i \cap K^2| = 0$. Set $V_i = \{\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}\} \setminus \{\sqrt[m_i]{N_i}\}$, and let $m[i]$ be the product of all m_k such that $k \neq i$. Then $[K[V_i] : K] = m[i]$ by Lemma 2.7. Thus, $F[V_i]$ is linearly disjoint from K over F. It follows that $\sqrt{-1} \notin F[V_i]$. For if $\sqrt{-1} \in F[V_i]$, then from $-1 \notin F^2$, we deduce that $1, \sqrt{-1}$ are F-linearly independent elements from $F[V_i]$, and hence K-linearly independent elements from $K[V_i]$, which cannot be as $4|m$. Since $M \in -D^2$, we have $F[\sqrt{-1}] = F[\sqrt{M}]$. Thus, $\sqrt{M} \notin F[V_i]$ and therefore $\sqrt{N_i} \notin F[V_i]$. If there is some $i \in M^\sharp$ such that $m_i = 2$, this shows that (1.1) holds. If, on the other hand, $4|m_i$ for all $i \in M^\sharp$, then (1.1) holds if and only if (1.4) fails, as in the proof of Lemma 2.8.

Suppose next that $|\mathcal{S}_2^i \cap K^2| = 1$ and let $N \in S_2^i \cap K^2$. Note that $N \notin -D^2$. We have $N = N_1^{g_1} \cdots N_\ell^{g_\ell}$, where $g_i = 0$, $0 \leq g_j < 2$ and $N^\sharp = \{j \in J \mid g_j = 1\}$ is nonempty. Fix any $j \in N^\sharp$ and let $S_2^{i,j}$ stand for the analogue of S_2 corresponding to $\{N_1, \dots, N_\ell\} \setminus \{N_i, N_j\}$. It is then clear that $S_2^{i,j} \cap K^2 = \emptyset$. Set $V_{i,j} = \{\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}\} \setminus \{\sqrt[m_i]{N_i}, \sqrt[m_j]{N_j}\}$, and let $m[i]$ (resp. $m[i,j]$) be the product of all m_k such that $k \neq i$ (resp. $k \neq i, j$). Then $[K[V_{i,j}] : K] = m[i,j]$ by Lemma 2.7. As above, we deduce that $\sqrt{-1} \notin F[V_{i,j}]$. Since $4|m$ and $S_2^i \cap (-D^2) = \emptyset$, Lemma 2.8 ensures that $[F[V_i] : F] = m[i]$ as well as $\sqrt{\pm N_j} \notin F[V_{i,j}]$. We deduce from Lemma 2.2 that $\sqrt{-1} \notin F[V_i]$. The rest of the argument follows as in the above case. ■

4 Primitive Elements

Isaacs [I] considered the problem of when $F[\alpha, \beta] = F[\alpha + \beta]$ for algebraic separable elements α, β of degrees m, n over F. He proved that if $[F[\alpha, \beta] : F] = mn$ (he actually assumed $\gcd(m, n) = 1$ but used only the stated condition) but $F[\alpha, \beta] \neq F[\alpha + \beta]$, then F has prime characteristic p, and the following conditions hold: $p|mn$ or $p < \min\{m, n\}$; if m, n are prime powers, then $p|mn$; p divides the order of the Galois group of a normal closure of $F[\alpha, \beta]$.

The condition $p < \min\{m, n\}$ was later improved to $p < \min\{m, n\}/2$ by Diviš [D].

Using Isaacs' result, we readily see that

$$F[\sqrt[m_1]{N_1}, \dots, \sqrt[m_\ell]{N_\ell}] = F[b_1 \sqrt[m_1]{N_1} + \cdots + b_\ell \sqrt[m_\ell]{N_\ell}]$$

for any nonzero $b_1, \dots, b_\ell \in F$ in Theorems 1.1, 1.2, and 1.3, provided the following conditions hold: $c(F) \neq p$ and $\mathcal{S}_p \cap D^p = \emptyset$ in Theorem 1.1; $c(F) \neq 2$, $\mathcal{S}_2 \cap D^2 = \emptyset$, and $(N_1, \dots, N_\ell)$ is not 2-defective in Theorem 1.2; $c(F) \nmid m\varphi(m)$ (Euler's function), $\mathcal{S}_2 \cap D^p = \emptyset$ for all $p \in \mathcal{P}$, and $(N_{i(2,1)}, \dots, N_{i(2,\ell(2))})$ is not 2-defective in Theorem 1.3.

It is actually possible that $F[\alpha, \beta]/F$ be a finite Galois extension, that $[F[\alpha, \beta] : F] = [F[\alpha] : F][F[\beta] : F]$, and still $F[\alpha, \beta] \neq F[\alpha + \beta]$. A family of examples can be found in [CS, Example 2.3].

References

[A] T. Albu, *Kummer extensions with few roots of unity*. J. Number Theory **41**(1992), 322–358. https://doi.org/10.1016/0022-314X(9)90131-8

[B] A. S. Besicovitch, *On the linear independence of fractional powers of integers*. J. Lond. Math. Soc. **15**(1940) 3–6. https://doi.org/10.1112/jlms/s1-15.1.3

[CS] L. Cagliero and F. Szechtman, *On the theorem of the primitive element with applications to the representation theory of associative and Lie algebras*. Canad. Math. Bull. 57(2014), 735–748. https://doi.org/10.4153/CMB-2013-046-9

[C] A. Capelli, *Sulla riduttibilitá delle equazioni algebriche. Nota prima*. Rend. Accad. Sci. Fis. Mat. Soc. Napoli 3(1897), 243–252.

[CO] R. Carr and C. O'Sullivan, *On the linear independence of roots*. Int. J. Number Theory 5(2009), 161–171. https://doi.org/10.1142/S1793042109002018

[D] B. Diviš, *On the degrees of the sum and product of two algebraic elements*. In: Number theory and algebra, Academic Press, New York, 1977, pp. 19–27.

[F] H. Flanders, *Advanced problems and solutions: Solutions 4797*. Amer. Math Monthly **67**(1960), 188–189.

[H] H. Hasse, *Klasssenkörpertheorie*. Mimeographed lectures, Marburg, 1932–33, pp. 187–195.

[I] I. M. Isaacs, *Degrees of sums in a separable field extension*. Proc. Amer. Math. Soc. **25**(1970), 638–641. https://doi.org/10.2307/2036661

[M] L. J. Mordell, *On the linear independence of algebraic numbers*. Pacific J. Math. **3**(1953), 625–630.

[R] L. Rédei, *Algebra*, *Vol. 1*. Pergamon Press, Oxford, 1967.

[Ri] I. Richards, *An application of Galois theory to elementary arithmetic*. Adv. in Math. **13**(1974) 268–273. https://doi.org/10.1016/0001-8708(74)90070-X

[Ro] R. L. Roth, *On extension of* $\mathbb{Q}$ *by square roots.* Amer. Math Monthly **78**(1971), 392–393. https://doi.org/10.2307/2316910

[S] C. L. Siegel, *Algebraische Abhängigkeit von Wurzein*. Acta Arith. **21**(1972), 59–64. https://doi.org/10.4064/aa-21-1-59-64

[U] H. D. Ursell, *The degree of radical extensions*. Canad. Math. Bull. **17**(1974), 615–617. https://doi.org/10.4153/CMB-1974-114-x

[V] K. T. Vahlen, *Über reductible Binome*. Acta Math. **19**(1895), 195–198. https://doi.org/10.1007/BF02402875

[Vi] I. M. Vinogradov, *Elements of number theory*. Dover, New York, 2016.

[Z] J.-P. Zhou, *On the degree of extensions generated by finitely many algebraic numbers*. J. Number Theory **34**(1990), 133–141. https://doi.org/10.1016/0022-314X(90)90144-G

Department of Mathematics and Statistics, University of Regina, Regina, SK, Canada
e-mail: fernando.szechtman@gmail.com

https://doi.org/10.4153/S0008439520000909 Published online by Cambridge University Press