BULL. AUSTRAL. MATH. SOC. 12F10, 12F99, 12G05
VOL. 64 (2001) [107–119]

RADICAL EXTENSIONS AND CROSSED HOMOMORPHISMS

FERNANDO BARRERA-MORA AND PABLO LAM-ESTRADA

If Ω/F is a Galois extension with Galois group G and $\mu(\Omega)$ denotes the group of roots of unity in Ω, we use the group $Z^1(G, \mu(\Omega))$ of crossed homomorphisms to study radical extensions inside Ω. Furthermore, we characterise cubic radical extensions, and we provide an example to show that this result can not be extended for higher degree extensions.

1. INTRODUCTION

In the last decade, several authors [**1, 3, 4**] have approached the study of radical extensions by using the group of one cocycles or crossed homomorphisms. More precisely, in [4] Barrera and Vélez proved a result, [**4**, Theorem 2.1] which characterises the radical subextensions inside a finite Galois extension, as those subfields associated, under the Galois correspondence, to subgroups which are kernels of crossed homomorphisms. Another connection between crossed homomorphisms and radical extensions occurs in a Theorem of Dummit, which has been extended in [**3**]. This result establishes an isomorphism from $Z^1(G, \mu(K))$ to $\operatorname{cog}(K/F) = T(K/F)/F^*$, where K/F is a Galois extension, $\mu(K)$ denotes the group of roots of unity in K and $T(K/F) := \{\alpha \in K \mid \alpha^n \in F \text{ for some } n \geqslant 1\}$. The mentioned results, show a close connection between the group of one cocycles and the radical extensions inside a Galois extension.

In this paper we present some results characterising radical extensions inside a Galois extension, using as a main tool the group of crossed homomorphisms. Also, using previous results on radical extensions, we are able to characterise cubic fields which are radical extensions and show by an example that this result can not be extended to extensions of higher degree.

2. NOTATION, TERMINOLOGY AND PRELIMINARY RESULTS

Given a field F, $F^* = F \setminus \{0\}$ will denote the group of nonzero elements in F, $\mu(F)$ denotes the group of roots of unity in F, and for a given n, $\mu_n(F)$ denotes the group of n-th roots of unity in F. When this group has order n, ζ_n will denote a fixed generator and it

Received 11th October, 2000
The authors were partially supported by COFFA-IPN and SNI-SEP.

will be called a primitive n-th root of unity. If K/F is a Galois extension (finite or infinite), then $G = \mathrm{Gal}(K/F)$, equipped with the Krull's topology, is a compact topological group. We shall consider $\mu(K)$ as a discrete topological group. A *crossed homomorphism* of G with coefficients in $\mu(K)$ is a continuous function $\chi : G \to \mu(K)$ which satisfies $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)^{\sigma}$, for every σ and τ in G. The set of all crossed homomorphisms of G with coefficients in $\mu(K)$ will be denoted by $Z^1\big(G, \mu(K)\big)$. For a given element $\zeta \in \mu(K)$, the function, which is assumed to be continuous, given by $\chi_\zeta(\sigma) = \sigma(\zeta)\zeta^{-1}$ is called an *inner crossed homomorphism* or a coboundary. The set of all inner crossed homomorphisms is denoted by $B^1\big(G, \mu(K)\big)$. We have that $B^1\big(G, \mu(K)\big) \leqslant Z^1\big(G, \mu(K)\big)$. If K/F is a field extension, we set $\mathrm{cog}(K/F) = T(K/F)/F^*$, where $T(K/F) = \{\alpha \in K \mid \alpha^n \in F \text{ for some } n \geqslant 1\}$. If a is a nonzero element of the field F, $\sqrt[n]{a}$ will denote a fixed root of $x^n - a$ in the algebraic closure of F. For an odd prime p, we shall denote by $F_{p(p-1)}$ the holomorph of the cyclic group of order p and we shall call it the Frobenius group of order $p(p-1)$.

DEFINITION 2.1: A finite field extension K/F is called a radical extension of exponent dividing n, if there exists a finite subgroup Δ/F^* of $\mathrm{cog}(K/F)$ of exponent dividing n so that $K = F(\Delta)$. If Δ/F^* is cyclic, K/F is called a simple radical extension.

Thus, K/F is a simple radical extension, or simply radical extension, if there exists $a \in F$ so that $K = F(\sqrt[n]{a})$ for some $n \in \mathbb{N}$.

DEFINITION 2.2: We say that the extension K/F has the *unique subfield property*, if for every m dividing the degree $[K : F]$, there exists a unique subfield of K/F whose degree over F is m.

THEOREM 2.1. [4, Theorem 1.5] *Let $x^n - a$ be irreducible over F, with $\mathrm{char}\, F$ not dividing n, and let α be a root of $x^n - a$. Then the extension $F(\alpha)/F$ has the unique subfield property if and only if*

(i) *for every odd prime p dividing n, $\zeta_p \notin F(\alpha) \setminus F$, and*
(ii) *if $4 \mid n$, then $\zeta_4 \notin F(\alpha) \setminus F$.*

COROLLARY 2.1. *Let F be a real field, $a \in F$ so that $x^n - a$ is irreducible over F and $\sqrt[n]{a} \in \mathbb{R}$. Then the extension $F(\sqrt[n]{a})/F$ has the unique subfield property.*

THEOREM 2.2. [4, Theorem 1.6] *Let F be a field such that $\mathrm{char}\, F$ does not divide n, $\zeta_n \in F$ and $x^n - a$, $x^n - b$ are irreducible over F. Then $F(\sqrt[n]{a}) = F(\sqrt[n]{b})$ if and only if $a = b^i c^n$, where $\gcd(i, n) = 1$ and $c \in F$.*

THEOREM 2.3. [4, Theorem 2.3] *Let K/F be a separable extension of degree n with Ω the Galois closure of K/F. Suppose that $\mathrm{char}\, F$ does not divide n and there exists a finite extension L/F with the following properties:*

(a) $\Omega(\zeta_n) \cap L = F$.
(b) $LK = L(\sqrt[n]{\alpha})$ *for some* $\alpha \in L$.

Then $K = F(\sqrt[n]{a})$ for some $a \in F$.

We need a bit of terminology to state the following theorem.

Let K/F be a separable extension of degree n. Asssume that (i) $\operatorname{char} F$ does not divide n, (ii) $K \cap F(\zeta_n) = F$, (iii) $K(\zeta_n)/F(\zeta_n)$ is cyclic and $K(\zeta_n)/F$ is Galois. Let $\Omega = K(\zeta_n)$. From Kummer Theory we have that $\Omega = L(\sqrt[n]{\alpha})$, where $L = F(\zeta_n)$ and $\alpha \in L$. By Theorem 2.2, we have that if $\sigma \in H = \operatorname{Gal}(K(\zeta_n)/K)$ then $\sigma(\alpha) = \gamma^n \alpha^{b_\sigma}$, where $\gamma \in L$ and $(b_\sigma, n) = 1$. Therefore $\sigma(\sqrt[n]{\alpha}) = \zeta_n^{i_\sigma} \gamma (\sqrt[n]{\alpha})^{b_\sigma}$ for some i_σ. Then with $\langle \tau \rangle = \operatorname{Gal}(\Omega/L)$, $\tau(\sqrt[n]{\alpha}) = \zeta_n \sqrt[n]{\alpha}$ we have that $\sigma^{-1} \tau \sigma = \tau^{a_\sigma^{-1} b_\sigma}$ where $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$ and from this, one concludes that

$$\sigma \tau \sigma^{-1} = \tau^{a_\sigma b_\sigma^{-1}}$$

With the previous notation we have:

THEOREM 2.4. [4, Theorem 2.4] *Let K/F be a separable extension of degree n so that $\operatorname{char} F$ and n are relatively prime. Set $H = \operatorname{Gal}\big(K(\zeta_n)/K\big)$. Assume:*

(a) $K \cap F(\zeta_n) = F$.

(b) *$K(\zeta_n)/F(\zeta_n)$ is cyclic with Galois group $\operatorname{Gal}\big(K(\zeta_n)/F(\zeta_n)\big) = \langle \tau \rangle$.*

Then

(i) *$K(\zeta_n)/F$ is normal. Moreover, $K(\zeta_n)/F$ is Abelian if and only if K/F is cyclic.*

(ii) *$\sigma\tau\sigma^{-1} = \tau^{a_\sigma b_\sigma^{-1}}$, for some integers a_σ, b_σ, and for every $\sigma \in H$.*

(iii) *K/F is radical if and only if $b_\sigma \equiv 1 \pmod{n}$, for all $\sigma \in H$.*

THEOREM 2.5. [4, Proposition 2.6] *Let K/F be an extension of degree p, p a rational prime different from $\operatorname{char} F$, and suppose that* (i) *$F(\zeta_p)/F$ is a quadratic extension,* (ii) *the Galois closure of K over F is $K(\zeta_p)$ and* (iii) *$\operatorname{Gal}\big(K(\zeta_p)/F\big) = D_p = \langle \tau, \sigma : \tau^p = \sigma^2 = 1, \sigma\tau\sigma^{-1} = \tau^{-1} \rangle$. Then K/F is a radical extension.*

COROLLARY 2.2. [4, Corollary to Proposition 2.6] *Let K/F be a cubic extension with the property that $K(\zeta_3)$ is the Galois closure of K over F and $\operatorname{char} F \neq 3$. Then K/F is radical.*

DEFINITION 2.3: An extension K/F is said to be a repeated radical extension, if there exists a sequence of fields $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$ so that F_{i+1}/F_i is radical for all $i = 0, \ldots, r-1$. In addition, if $[F_{i+1} : F_i] = n_i$, where $F_{i+1} = F_i(\sqrt[n_i]{a_i})$, for some $a_i \in F_i$, and for all $i = 0, \ldots, r-1$, then K/F is said to be a radical tower; if $r = 1$, then K/F is said to be a simple radical tower.

THEOREM 2.6. [2, Theorem 3.4] *Let Ω/F be a repeated radical Galois extension and suppose that $\Omega \setminus F$ contains no pth root of unity for any prime p. Then F contains a primitive pth root of unity for every prime divisor of $[\Omega : F]$.*

THEOREM 2.7. (Hilbert's Theorem 90) *Let K/F be a Galois extension (finite or infinite). Then $Z^1(G, K^*) = B^1(G, K^*)$.*

3. Radical Subfields inside a Galois Extension

Studying radical extensions when enough roots of unity are present in the ground field is done by Kummer Theory, hence it is natural to consider the case when the ground field lacks enough roots of unity.

In what follows we assume that for a given positive integer n, the ground field F does not contain a primitive n-th root of one.

Let n be a positive integer, F a field whose characteristic does not divide n. Let $\Omega_n = F\big(\zeta_n, \sqrt[n]{F(\zeta_n)}\big)$. Then Ω_n is the splitting field of $\mathcal{F}_n = \big\{f_\alpha(x^n) : f_\alpha(x) = \operatorname{irr}(\alpha, F),\ \alpha \in F(\zeta_n)\big\}$ over F, hence Ω_n/F is a Galois extension, in general infinite. If Γ_n denotes the Galois group of Ω_n/F, it is endowed with Krull's topology. Since $F(\zeta_n)/F$ is normal, we have that $\operatorname{Gal}\big(\Omega_n/F(\zeta_n)\big)$ is a normal subgroup of Γ_n, and the short exact sequence

$$1 \longrightarrow \operatorname{Gal}\big(\Omega_n/F(\zeta_n)\big) \longrightarrow \Gamma_n \longrightarrow \operatorname{Gal}\big(F(\zeta_n)/F\big) \longrightarrow 1.$$

A result of Dummit states that if K/F is a Galois extension, then $\operatorname{cog}(K/F) \cong Z^1\big(G, \mu(K)\big)$. The isomorphism induces a one to one correspondence between the lattice of subgroups of $\operatorname{cog}(K/F)$ and $Z^1\big(G, \mu(K)\big)$. The correspondence is given by

$$\phi : \big\{\Delta \mid F^* \leqslant \Delta \leqslant T(K/F)\big\} \longrightarrow \Big\{U \mid U \leqslant Z^1\big(G, \mu(K)\big)\Big\}$$
$$\phi(\Delta) = \Big\{\chi_\alpha \in Z^1\big(G, \mu(K)\big) \mid \alpha \in \Delta\Big\},$$

where $\chi_\alpha(\sigma) = \sigma(\alpha)/\alpha$. With the assumptions as above, there is a map

$$B : G \times Z^1\big(G, \mu(K)\big) \longrightarrow \mu(K)$$
$$B(\sigma, \chi) = \chi(\sigma).$$

Given a subgroup $U \leqslant Z^1\big(G, \mu(K)\big)$ we define $U^\perp = \big\{\sigma \in G \mid \chi(\sigma) = 1, \text{for all } \chi \in U\big\}$. If U is cyclic generated by χ (in the algebraic sense), we shall use the notation $U^\perp = \chi^\perp$ and call it the *kernel* of χ. Notice that this is an open subgroup of G.

The next result establishes a connection between these subgroups and the finite radical extensions inside Ω_n.

The following theorem generalises [4, Theorem 2.1]

Theorem 3.1. *Let K/F be a finite extension contained in Ω_n. Then K/F is a simple radical extension of exponent dividing n if and only if $\operatorname{Gal}(\Omega_n/K) = \chi^\perp$ for some $\chi \in Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$.*

Proof: Assume that K/F is a simple radical of exponent dividing n. Then there exists $\alpha \in \Omega_n$ so that $\alpha^n \in F$ and $K = F(\alpha)$. Define $\chi_\alpha : \Gamma_n \to \mu_n(\Omega_n)$ by $\chi_\alpha(\sigma) = \sigma(\alpha)/\alpha$. It would be clear that $\chi_\alpha \in Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$, provided that χ_α is continuous. Let $\zeta \in \mu_n(\Omega_n)$. We shall prove that $\chi_\alpha^{-1}(\zeta)$ is an open subset in Γ_n. We may assume

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

$\chi_\alpha^{-1}(\zeta)$ is not empty and let $\sigma \in \chi_\alpha^{-1}(\zeta)$, that is, $\sigma(\alpha) = \zeta\alpha$. Let $\overline{K}$ be the normal closure of K which is necessarily contained in Ω_n, and $\mathrm{Gal}(\Omega_n/\overline{K}) \leqslant \mathrm{Gal}(\Omega_n/K)$. Given $\rho \in \mathrm{Gal}(\Omega_n/\overline{K})$, we have that $\chi_\alpha(\rho) = 1$, and hence $\chi_\alpha(\sigma\rho) = \zeta$ hence $\sigma\rho \in \chi_\alpha^{-1}(\zeta)$. Therefore, $\sigma\,\mathrm{Gal}(\Omega_n/\overline{K}) \subseteq \chi_\alpha^{-1}(\zeta)$, and $\mathrm{Gal}(\Omega_n/K) = \chi_\alpha^\perp$.

Assume now that $\mathrm{Gal}(\Omega_n/K) = H = \chi^\perp$, for some $\chi \in Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$. Then H is open and closed, hence $[\Gamma_n : H] < +\infty$, since Γ_n is compact. Let $K = \Omega_n^H$, since H is closed then $\mathrm{Gal}(\Omega_n/K) = \overline{H} = H$. From Hilbert's Theorem 90 (Theorem 2.7), we have $\chi \in Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big) = B^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$. Therefore there exists $\alpha \in \Omega_n^*$ so that $\chi = \chi_\alpha$, that is $\chi_\alpha(\sigma) = \chi(\sigma) = \sigma(\alpha)/\alpha$, for every $\sigma \in \Gamma_n$. Let $\sigma_1, \ldots, \sigma_t \in \Gamma_n$ be the representatives of left cosets of H in Γ_n. Since $\sigma_i(\alpha)/\alpha \in \mu_n(\Omega_n)$ for every $i = 1, \ldots, t$, there exists m dividing n so that $\big[\sigma_i(\alpha)/\alpha\big]^m = 1$ for every i. Given $\sigma \in \Gamma_n$, $\sigma = \sigma_i\tau$ for some i and some $\tau \in H$, we have $\sigma(\alpha^m) = \alpha^m$ for every $\sigma \in \Gamma_n$, then $\alpha^m \in F$. The equivalence $\tau(\alpha)/\alpha = 1$ if and only if $\tau \in H = \chi^\perp$, guarantees $K = F(\alpha)$ since H is closed, that is K is a simple radical of exponent dividing n. □

THEOREM 3.2. *Let K/F be a finite extension, $K \leqslant \Omega_n$. Then K/F is a radical extension of exponent dividing n if and only if there exists a subgroup $U \leqslant Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$ so that $\mathrm{Gal}(\Omega_n/K) = U^\perp$.*

PROOF: Assume $K = F(\Delta)$, where Δ/F^* is a finite subgroup of $\mathrm{cog}(K/F)$ of exponent dividing n, and let $U = \{\chi_\alpha \mid \alpha \in \Delta\}$. One verifies that U is a subgroup of $Z^1\big(\Gamma_n, \mu_n(\Omega_n)\big)$. We have, $U^\perp = \bigcap_{\chi \in U} \chi^\perp$. We also have that every $\chi \in U$ is continuous (previous theorem) and $\chi^\perp = \chi^{-1}(1)$. Thus $\chi^\perp$ is open and closed. Therefore $U^\perp$ is a closed subgroup of Γ_n. We also have that the relation $\sigma \in U^\perp$ is equivalent to $\sigma(\alpha)/\alpha = \chi_\alpha(\sigma) = 1$ for every $\alpha \in \Delta$, that is $\sigma(\alpha) = \alpha$ for every $\alpha \in K$, or equivalently $\sigma \in \mathrm{Gal}(\Omega_n/K)$, so $\mathrm{Gal}(\Omega_n/K) = U^\perp$.

Conversely, assume there exists $U \leqslant Z^1\big(\Gamma_n, \mu(\Omega_n)\big)$ so that $\mathrm{Gal}(\Omega_n/K) = U^\perp$. Let $\Delta = \{\alpha \in \Omega_n \mid \chi_\alpha \in U\}$.

It is straightforward to show that Δ is a subgroup of Ω_n^*. Since K/F is finite then $U^\perp$ is open in Γ_n, so compactness of Γ_n implies $[\Gamma_n : U^\perp] < +\infty$, actually $U^\perp$ is open and closed. Let $\tau_1, \ldots, \tau_t$ be a set of representatives of the left cosets of $U^\perp$ in Γ_n, hence given $\sigma \in \Gamma_n$, $\sigma = \tau_i\rho$ for some i and some $\rho \in U^\perp$. If $\alpha \in \Delta$ then $\chi_\alpha(\sigma) \in \mu(\Omega_n)$ implies that there exists $n_\sigma \in \mathbb{N}$ so that $\big[\sigma(\alpha)/\alpha\big]^{n_\sigma} = 1$. Since $\rho \in U^\perp$, it follows that $\chi_\alpha(\sigma) = \chi_\alpha(\tau_i\rho) = \chi_\alpha(\tau_i)\tau_i\chi_\alpha(\rho) = \chi_\alpha(\tau_i)$. Hence $\big[\sigma(\alpha)/\alpha\big]^{n_i} = \big[\tau_i(\alpha)/\alpha\big]^{n_i} = 1$, for some $n_1, \ldots, n_t$ positive integers. Let $N = \mathrm{lcm}\{n_1, \ldots, n_t\}$. Then $\big[\sigma(\alpha)/\alpha\big]^N = \sigma(\alpha^N)/\alpha^N = 1$, for every $\sigma \in \Gamma_n$. Thus $\alpha^N \in F$, that is $\Delta \leqslant T(\Omega_n/F)$. It is clear that $F(\Delta)$ is the fixed field of $U^\perp$ and since $U^\perp$ is closed and $U^\perp = \mathrm{Gal}(\Omega_n/K)$, then $K = F(\Delta)$. □

When studying radical extensions $F(\alpha)/F$, where $\alpha^n \in F$ for some positive integer n, it is important to know when the order of αF^* is equal to the degree $\big[F(\alpha) : F\big]$. Also,

in solving various problems related to radical extensions, it might be the case that a field extension is not radical, but a repeated radical extension. The question is: How can we use crossed homomorphisms to determine if a given extension is a repeated radical extension? The next result goes into that point.

THEOREM 3.3. *Let E/F be a finite and separable extension of degree n so that* char F *does not divide n. Let Ω be the Galois closure of the extension $E(\zeta_n)$ over F with $G = \mathrm{Gal}(\Omega/F)$ and $H = \mathrm{Gal}(\Omega/E)$. Let $K = E \cap F(\zeta_n)$. Then E/K is a radical tower if and only if there exists a tower of fields*

$$L_0 = F(\zeta_n) \subseteq L_1 \subseteq \cdots \subseteq L_r = E(\zeta_n)$$

such that

(i) $\sigma(L_i) = L_i$ *for each* $\sigma \in H$ *and for all* $i = 0, \ldots, r$,

(ii) L_{i+1}/L_i *is a cyclic extension for all* $i = 0, \ldots, r-1$,

(iii) *if* $\mathrm{Gal}(L_{i+1}/L_i) = \langle \tau_i \rangle$ *and* $d_i = [L_{i+1} : L_i]$, *then* $\langle \tau_i \rangle$ *is H-isomorphic to* $\langle \zeta_{d_i} \rangle$ *where H acts by conjugation over* $\langle \tau_i \rangle$ *under restriction and by canonical action over* $\langle \zeta_{d_i} \rangle$ *for all* $i = 0, \ldots, r-1$.

PROOF: Observe that $E(\zeta_n)/E$ is a Galois extension with $\mathrm{Gal}\big(E(\zeta_n)/E\big) \cong \mathrm{Gal}\big(F(\zeta_n)/K\big)$. Therefore $\big[E(\zeta_n) : E\big] = \big[F(\zeta_n) : K\big]$ and $\big[E(\zeta_n) : F(\zeta_n)\big] = [E : K]$.

We assume that E/K is a radical tower. Let $K_0 = K \subseteq K_1 \subseteq \cdots \subseteq K_r = E$ be a tower of fields such that for all $i = 0, \ldots, r-1$, there exists $\beta_i \in K_{i+1}$ such that $K_{i+1} = K_i(\beta_i)$ with $\beta_i^{d_i} \in K_i$ where $d_i = [K_{i+1} : K_i]$. Let $L_i = K_i(\zeta_n)$ for all $i = 0, \ldots, r$. We have that $K_i F(\zeta_n) = L_i$ with $K_i \cap F(\zeta_n) = K$ for which $\mathrm{Gal}(L_i/K_i) \cong \mathrm{Gal}\big(F(\zeta_n)/K\big)$. Then $[L_i : K_i] = \big[F(\zeta_n) : K\big]$ and $d_i = [K_{i+1} : K_i] = [L_{i+1} : L_i]$. Since $K_i \subseteq E = \Omega^H$ and $L_{i+1} = K_{i+1}(\zeta_n) = K_i(\zeta_n)(\beta_i) = L_i(\beta_i)$ with $\beta_i^{d_i} \in K_i \subseteq L_i$, we obtain that $\sigma(L_i) = L_i$ for all $\sigma \in H$ and L_{i+1}/L_i is a cyclic extension. Therefore, (i) and (ii) of the theorem hold. Now we establish (iii). Let τ_i be a generator of the Galois group of the extension L_{i+1}/L_i such that $\tau_i(\beta_i) = \zeta_{d_i}\beta_i$. Let $\sigma \in H$ and we write $\sigma(\zeta_{d_i}) = \zeta_{d_i}^{a_\sigma}$ for some a_σ. Then, $\sigma(\beta_i) = \beta_i$ and $\sigma\tau_i\sigma^{-1}|_{L_{i+1}} \in \mathrm{Gal}(L_{i+1}/L_i)$ where $(\sigma\tau_i\sigma^{-1})(\beta_i) = \zeta_{d_i}^{a_\sigma}\beta_i = \tau_i^{a_\sigma}(\beta_i)$, that is, $\sigma\tau_i\sigma^{-1}|_{L_{i+1}} = \tau_i^{a_\sigma}$. Therefore, we have (iii).

Conversely, assume the conditions. By Kummer Theory, there exists $\alpha_i \in L_{i+1}$ such that $L_{i+1} = L_i(\alpha_i)$ with $\mathrm{irr}(\alpha_i, L_i) = x^{d_i} - a_i$ ($a_i \in L_i$). Let $\tau_i \in \mathrm{Gal}(L_{i+1}/L_i)$ be such that $\tau_i(\alpha_i) = \zeta_{d_i}\alpha_i$. For each element $\sigma \in H$, we write $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$ with $(a_\sigma, n) = 1$, and hence $\sigma(\zeta_{d_i}) = \zeta_{d_i}^{a_\sigma}$. Since $\sigma(L_i) = L_i$ (for all $i = 0, \ldots, r$), we have that $L_{i+1} = L_i(\alpha_i) = L_i\big(\sqrt[d_i]{\sigma(a_i)}\big)$. By Theorem 2.2, $\sigma(a_i) = \gamma_\sigma^{d_i} a_i^{b_\sigma}$ with $\gamma_\sigma \in L_i$ and $(b_\sigma, d_i) = 1$. Hence,

$$\sigma(\alpha_i) = \zeta_{d_i}^{i_\sigma}\gamma_\sigma\alpha_i^{b_\sigma} \tag{1}$$

for some i_σ. Let $M_i = \mathrm{Gal}(\Omega/L_i)$ (for each $i = 0, \ldots, r$). We have that $M_{i+1} \lhd M_i$ with $\mathrm{Gal}(L_{i+1}/L_i) = M_i/M_{i+1}$. Also $\sigma M_i \sigma^{-1} = M_i$, since $\sigma(L_i) = L_i$. Extending τ_i to

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

a L_i–automorphism of Ω, we have that $\sigma\tau_i\sigma^{-1} \in M_i$. Moreover, it is easy to check that $\sigma\tau_i\sigma^{-1}|_{L_{i+1}} = \tau_i^{a_\sigma b_\sigma^{-1}}$. From (iii), we must have that

$$b_\sigma \equiv 1 \bmod d_i \tag{2}$$

that is $\sigma\tau_i\sigma^{-1}|_{L_{i+1}} = \tau_i^{a_\sigma}$ for each $\sigma \in H$. Thus $H < \mathrm{N}_G(M_i)$ and $HM_i < \mathrm{N}_G(M_i)$. Let $K_i = \Omega^{HM_i}$ for each $i = 0, \dots, r$. Then we have the tower of fields $K_0 = K \subseteq K_1 \subseteq \cdots \subseteq K_r = E$. Since L_{i+1}/L_i is a radical extension, we choose $\chi_i \in Z^1\big(M_i, \mu(\Omega)\big)$ so that $\chi_i^\perp = M_{i+1}$ and $\chi_i(\theta) = \theta(\alpha_i)/\alpha_i$ for each $\theta \in M_i$ (Theorem 3.1). We define $\overline{\chi_i} : HM_i \longrightarrow \mu(\Omega)$ given by $\overline{\chi_i}(\sigma\theta) := \sigma\big(\chi_i(\theta)\big)$ for each $\sigma \in H$ and for each $\theta \in M_i$.

Firstly $\overline{\chi_i}$ is well defined. If $\sigma, \sigma_1 \in H$ and $\theta, \theta_1 \in M_i$ with $\sigma\theta = \sigma_1\theta_1$, then $\sigma_1^{-1}\sigma = \theta_1\theta^{-1} \in H \cap M_i = \mathrm{Gal}(\Omega/EL_i) = \mathrm{Gal}\big(\Omega/E(\zeta_n)\big) = M_r \subseteq M_{i+1}$. This implies that $\theta(\alpha_i) = \theta_1(\alpha_i)$ and $\sigma(\zeta) = \sigma_1(\zeta)$ for any nth root of unity ζ. Therefore

$$\sigma\big(\chi_i(\theta)\big) = \sigma\left(\frac{\theta(\alpha_i)}{\alpha_i}\right) = \sigma\left(\frac{\theta_1(\alpha_i)}{\alpha_i}\right) = \sigma_1\left(\frac{\theta_1(\alpha_i)}{\alpha_i}\right) = \sigma_1\big(\chi_i(\theta_1)\big).$$

Secondly $\overline{\chi_i} \in Z^1\big(HM_i, \mu(\Omega)\big)$. In fact, we shall prove that for all $\delta, \gamma \in HM_i$

$$\overline{\chi_i}(\delta\gamma) = \delta\big(\overline{\chi_i}(\gamma)\big) \cdot \overline{\chi_i}(\delta) \tag{3}$$

We write $\delta = \sigma\theta$ and $\gamma = \sigma_1\theta_1$ where $\sigma, \sigma_1 \in H$ and $\theta, \theta_1 \in M_i$. By (1) and (2), we have that $\big(\sigma_1(\alpha_i)\big)/\alpha_i \in L_i$, and hence $\theta\big(\sigma_1(\alpha_i)/\alpha_i\big) = \big(\sigma_1(\alpha_i)/\alpha_i\big)$, equivalently

$$\frac{\theta\sigma_1(\alpha_i)}{\sigma_1(\alpha_i)} = \frac{\theta(\alpha_i)}{\alpha_i} \tag{4}$$

Let $\theta_2 = \sigma_1^{-1}\theta\sigma_1 \in M_i$. Then

$$\begin{aligned}
\overline{\chi_i}(\delta\gamma) &= \overline{\chi_i}(\sigma\theta\sigma_1\theta_1) = \overline{\chi_i}(\sigma\sigma_1\theta_2\theta_1) = \sigma\sigma_1\big(\chi_i(\theta_2\theta_1)\big) \\
&= \sigma\sigma_1\left(\frac{\theta_2\theta_1(\alpha_i)}{\alpha_i}\right) = \sigma\sigma_1\left(\frac{\sigma_1^{-1}\theta\sigma_1\theta_1(\alpha_i)}{\alpha_i}\right) \\
&= \sigma\left(\frac{\theta\sigma_1\theta_1(\alpha_i)}{\sigma_1(\alpha_i)}\right) = \sigma\left(\frac{\theta\sigma_1\theta_1(\alpha_i)}{\theta\sigma_1(\alpha_i)} \cdot \frac{\theta\sigma_1(\alpha_i)}{\sigma_1(\alpha_i)}\right) \\
&= \sigma\left(\theta\sigma_1\left(\frac{\theta_1(\alpha_i)}{\alpha_i}\right) \cdot \frac{\theta(\alpha_i)}{\alpha_i}\right) \text{ by (4)} \\
&= \sigma\theta\big(\sigma_1\chi_i(\theta_1)\big) \cdot \sigma\chi_i(\theta) = \sigma\theta\big(\overline{\chi_i}(\sigma_1\theta_1)\big) \cdot \overline{\chi_i}(\sigma\theta) \\
&= \delta\big(\overline{\chi_i}(\gamma)\big) \cdot \overline{\chi_i}(\delta).
\end{aligned}$$

Therefore, the relation (3) holds.

Finally $\overline{\chi_i}^\perp = HM_{i+1}$. We have that for $\sigma \in H$ and $\theta \in M_i$

$$\begin{aligned}
\sigma\theta \in \overline{\chi_i}^\perp &\iff 1 = \overline{\chi_i}(\sigma\theta) = \sigma\big(\chi_i(\theta)\big) \\
&\iff \chi_i(\theta) = 1 \iff \theta \in \chi_i^\perp = M_{i+1} \\
&\implies \sigma\theta \in HM_{i+1}
\end{aligned}$$

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

Hence $\overline{\chi_i}^{\perp} \subseteq HM_{i+1}$. Conversely, if $\sigma\theta \in HM_{i+1}$, then there exist $\sigma_1 \in H$ and $\theta_1 \in M_{i+1}$ such that $\sigma\theta = \sigma_1\theta_1$. Hence $\overline{\chi_i}(\sigma\theta) = \overline{\chi_i}(\sigma_1\theta_1) = \sigma_1\big(\chi_i(\theta_1)\big) = \sigma_1(1) = 1$. Therefore, $\sigma\theta \in \overline{\chi_i}^{\perp}$.

Thus we have proved that the extension K_{i+1}/K_i is radical for all i. Let $\beta_i \in K_{i+1}$ be such that $K_{i+1} = K_i(\beta_i)$ with $\overline{\chi_i}(\sigma\theta) = \big(\sigma\theta(\beta_i)/\beta_i\big)$ for each $\sigma \in H$ and $\theta \in M_i$. Observe that $L_i \cap K_{i+1} = \Omega^{M_i} \cap \Omega^{HM_{i+1}} = \Omega^{\langle M_i, HM_{i+1}\rangle} = \Omega^{HM_i} = K_i$, and $\big(\theta(\beta_i)/\beta_i\big) = \overline{\chi_i}(\theta) = \chi_i(\theta) = \theta(\alpha_i)/\alpha_i$ for each $\theta \in M_i$, that is, $\beta_i/\alpha_i \in L_i$. Let $b_i \in L_i$ be so that $\beta_i = b_i\alpha_i$. Then $\beta_i^{d_i} = b_i^{d_i}\alpha_i^{d_i} \in L_i \cap K_{i+1} = K_i$. Therefore $[K_{i+1} : K_i] \leqslant d_i$. Since

$$\prod_{i=0}^{r-1}[K_{i+1} : K_i] = [E : K] = \big[E(\zeta_n) : F(\zeta_n)\big] = \prod_{i=0}^{r-1}[L_{i+1} : L_i] = d_0 \cdots d_{r-1},$$

we have that $[K_{i+1} : K_i] = d_i$ with $x^{d_i} - \beta_i^{d_i} = \operatorname{irr}(\beta_i, K_i)$. Therefore the extension E/K is a radical tower. □

With analogous notation, to that of Theorem 2.4, we have:

COROLLARY 3.1. *Let E/F be a finite and separable extension of degree n so that* char F *does not divide n. Assume $E \cap F(\zeta_n) = F$ and $E(\zeta_n)/F(\zeta_n)$ is cyclic with Galois group generated by τ. Then, the following conditions are equivalent*

(i) *E/F is a radical extension.*

(ii) *$\sigma\tau\sigma^{-1} = \tau^{a_\sigma}$ for all $\sigma \in \operatorname{Gal}\big(E(\zeta_n)/E\big)$, where $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$.*

(iii) *E/F is a simple radical tower.*

PROOF: We have that $E(\zeta_n)/F$ is normal, and (i) is equivalent to (ii) [Theorem 2.4]. By Theorem 3.3, (ii) implies (iii). It is clear that (iii) implies (i). □

4. RIGHT NORMAL CLOSURE, NOT NECESSARILY RADICAL

It is well known that if K/F is a radical extension, say $K = F(\sqrt[r]{a})$, then the normal closure of K over F is $K(\zeta_n)$. A natural question is if the condition is also sufficient. In [4] (at the end of the paper), an example was given to show that with the above condition, K is not necessarily a radical extension of F. However, we shall see that for extensions of degree 3 over $\mathbb{Q}$, this condition is equivalent to one on the discriminant of the polynomial defining the field K, which is necessary and sufficient for K to be radical over $\mathbb{Q}$. We also present an example to show that in general, not only is K not radical, but K is not contained in a real repeated radical extension. This example also shows that the condition on p in the following theorem is necessary.

THEOREM 4.1. [5, Theorem 9.2] *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.*

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

THEOREM 4.2. *Let p be an odd prime, $f(x) \in \mathbb{Q}[x]$ an irreducible and solvable polynomial of degree p. Assume that $f(x)$ has only one real root α. Then there exists a real field L so that*

(i) $\mathbb{Q}(\alpha) \subseteq L$,

(ii) *L contains a subfield F so that $[L : F] = p$ and L/F is radical.*

PROOF: Since $f(x)$ is solvable of degree p, then its Galois group G_f is isomorphic to a subgroup of the Frobenius group $F_{p(p-1)} = C_p \rtimes C_{p-1}$. If Ω denotes the splitting field of $f(x)$, the condition $G_f \hookrightarrow F_{p(p-1)}$ guarantees the existence of a subfield K of Ω so that $K/\mathbb{Q}$ is cyclic and $[K : \mathbb{Q}]$ divides $p-1$. If α denotes the real root of $f(x)$ then $\Omega = K\mathbb{Q}(\alpha) = K(\alpha)$. We also have $\big[K(\zeta_p) : \mathbb{Q}\big]$ is relatively prime to p. Set $L = \mathbb{R} \cap \Omega(\zeta_p)$ and $F = \mathbb{R} \cap K(\zeta_p)$. We have $\alpha \in L$ and since f does not split in $\mathbb{R}$ neither it does in L. Hence $L/\mathbb{Q}$ is not normal, so $F \neq L$ (otherwise $L/\mathbb{Q}$ would be a subfield of an Abelian field, particularly normal over $\mathbb{Q}$).

Since $\Omega(\zeta_p)/\mathbb{Q}$ is normal, we have $L \neq \Omega(\zeta_p)$, moreover, $\big[\Omega(\zeta_p) : L\big] = 2$ and $[L : F] = p$. We have $L = F(\alpha)$ and $f(x)$ is irreducible over F. Thus L/F is not normal and the normal closure of L/F is $\Omega(\zeta_p) = L(\zeta_p)$. An easy calculation shows that $\mathrm{Gal}\big(L(\zeta_p)/F\big) = D_p$, the dihedral group of order $2p$. Applying Theorem 2.5 one concludes that L/F is a radical extension. □

THEOREM 4.3. *Let p be an odd prime and $f(x) \in \mathbb{Z}[x]$ a monic and irreducible polynomial of degree p. If α is a root of $f(x)$ and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is radical then the discriminant D_f of f is given by $D_f = (-1)^{p(p-1)/2} p m^2$ for some $m \in \mathbb{Z}$.*

PROOF: Assume $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[n]{a})$ with n minimum and $a \in \mathbb{Z}$. Let $\beta = \sqrt[n]{a}$ and $g(x) = \mathrm{irr}(\beta, \mathbb{Q})$, then $g(x)$ divides $x^n - a = \prod_{i=1}^{n}(x - \zeta_n^i \beta)$. If m is the degree of $g(x)$, then $\zeta_n^k \beta^m \in \mathbb{Q}$ for some $k \geqslant 1$. Also $\zeta_n^k \in \mathbb{Q}(\alpha)$. Let $\zeta_n^k = \zeta_l$. If $\zeta_l \notin \mathbb{Q}$ then $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_l)$, thus $p = \big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = \big[\mathbb{Q}(\zeta_l) : \mathbb{Q}\big] = \phi(l)$, however, $\phi(l)$ is prime only for $2 = \phi(l) = \phi(3)$. Since p is odd this is not possible. Hence $\zeta_l \in \mathbb{Q}$ and $\beta^m \in \mathbb{Q}$. The minimality of n implies $n = m$ and $g(x) = x^p - a$. We also have

$$\begin{aligned} D_g &= (-1)^{p(p-1)/2} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\big(g'(\beta)\big) = (-1)^{p(p-1)/2} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(p\beta^{p-1}) \\ &= (-1)^{p(p-1)/2} p^p N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)^{p-1} = (-1)^{p(p-1)/2} p(pa)^{p-1} = (-1)^{p(p-1)/2} p m^2, \end{aligned}$$

since $p - 1 \equiv 0 \pmod 2$. It is well known that if $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ with $f(\alpha) = g(\beta)$ with f and g irreducible polynomials, then $D_f = D_g m_1^2$ for some $m_1 \in \mathbb{Z}$. From this the conclusion follows. □

THEOREM 4.4. [5, Theorem 9.4] *Let $f(x) \in \mathbb{Z}[x]$ be a cubic irreducible monic polynomial and $K = \mathbb{Q}(\alpha)$ with $f(\alpha) = 0$. Then $K/\mathbb{Q}$ is radical if and only if $D_f = -3m^2$ for some $m \in \mathbb{Z}$.*

PROOF: The necessity follows immediately from the last theorem. Conversely, since $D_f = -3m^2$, it follows that ζ_3 belongs to the normal closure of $\mathbb{Q}(\alpha)$. Now apply

Corollary 2.2. □

THEOREM 4.5. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible cubic polynomial and $K = \mathbb{Q}(\alpha)$ with $f(\alpha) = 0$. If Ω denotes the normal closure of K over $\mathbb{Q}$, then the following statements are equivalent.*

(i) $\Omega = K(\zeta_3)$.

(ii) *$K/\mathbb{Q}$ is a radical extension.*

(iii) $D_f = -3m^2$, *for some* $m \in \mathbb{Z}$

PROOF: (i) $\Longleftrightarrow$ (ii) by Corollary 2.2. (ii) $\Longleftrightarrow$ (iii) by Theorem 4.4. □

Next, we shall use some terminology from cyclotomic fields, which is provided here.

Let p be an odd prime, $\mathbb{Q}(\zeta_p)$ the pth cyclotomic field. The elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ are: σ_a, $1 \leqslant a \leqslant p-1$, where $\sigma_a(\zeta_p) = \zeta_p^a$. As usual, $\mathbb{Q}(\zeta_p)^+$ will denote the maximal real field of $\mathbb{Q}(\zeta_p)$, and h and h^+ denote the class number of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_p)^+$ respectively. Let g be a fixed primitive root mod p and let i be an even integer, $2 \leqslant i \leqslant p-3$. Define

$$E_i = \prod_{a=1}^{p-1} \left(\zeta_p^{(1-g)/2} \frac{1-\zeta_p^g}{1-\zeta_p} \right)^{a^i \sigma_a^{-1}}$$

It is straightforward to show that E_i is a unit in $\mathbb{Q}(\zeta_p)^+$.

With the above notation the following theorem holds [6, Theorem 8.14].

THEOREM 4.6. *$p \mid h^+$ if and only if some E_i is a pth power of a unit of $\mathbb{Q}(\zeta_p)^+$.*

Let ζ denote a fixed primitive 7th root of unity, and let $K = \mathbb{Q}(\zeta)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta)$, that is, $K = \mathbb{Q}(\zeta + \zeta^{-1})$. If $\mathcal{O}_K$ and $\mathcal{U}_K$ denote the ring of integers of K and the group of units of $\mathcal{O}_K$ respectively, then by Dirichlet's Unit Theorem, $\mathcal{O}_K \cong \langle \pm 1 \rangle \times \langle u_1 \rangle \times \langle u_2 \rangle$, where u_1 and u_2 generate infinite cyclic groups. With the previous notation, we have:

LEMMA 4.1. *K is not contained in a real repeated radical extension.*

PROOF: We shall prove the assertion by contradiction. Assume K is contained in a real repeated radical extension. Choose one with minimum length. So we may assume that $\mathbb{Q} \subseteq M_1 \subseteq M_2 \subseteq \mathbb{R}$ is a tower of fields so that $M_1/\mathbb{Q}$ is a real repeated radical extension, $M_1 \cap K = \mathbb{Q}$, M_2/M_1 is radical $K \subseteq M_2$. We also have that all subfields of M_2/M_1 are radical (Corollary 2.1), hence the minimality of M_2 and $K/\mathbb{Q}$ being normal imply $[M_2 : M_1] = 3$. Note that $K(\zeta_3)/\mathbb{Q}$ is a cyclic extension of degree 6 and the only real subfield of $K(\zeta_3)/\mathbb{Q}$ is K which is not contained in M_1. Hence $M_1 \cap K(\zeta_3) = \mathbb{Q}$. From Theorem 2.3, we have that $K/\mathbb{Q}$ is a radical extension, a contradiction. □

LEMMA 4.2. *Let F_{42} be the Frobenius group of order 42. Then, F_{42} has at least two subgroups of order 3.*

THEOREM 4.7. *Let $u \in \mathcal{U}_K \cap \mathbb{R}$ be so that*

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

(i) $x^7 - u$ *is an irreducible polynomial over* $\mathbb{Q}(\zeta)$,

(ii) $\Omega/\mathbb{Q}$ *is a Galois extension, where* $\Omega = \mathbb{Q}(\zeta, \sqrt[7]{u})$ *and* $\sqrt[7]{u}$ *is the real root of* $x^7 - u$.

Then,

(a) $K(\sqrt[7]{u})/\mathbb{Q}$ *is not a Galois extension,*

(b) $\mathrm{Gal}(\Omega/\mathbb{Q}) \cong F_{42}$, *where* F_{42} *is the Frobenius group of order* 42,

(c) *there exists an extension* $F/\mathbb{Q}$ *of degree* 7, $F \subseteq \Omega$, *and* F *is not a radical extension over* $\mathbb{Q}$,

(d) $K(\sqrt[7]{u})/\mathbb{Q}$ *is not a real repeated radical extension,*

(e) *the normal closure of the extension* $F/\mathbb{Q}$ *is* Ω,

(f) F *is not contained in a real repeated radical extension.*

PROOF: Let $G = \mathrm{Gal}(\Omega/\mathbb{Q})$.

(a): If $K(\sqrt[7]{u})/\mathbb{Q}$ is a Galois extension, then, in particular, $K(\sqrt[7]{u})/K$ would be so. Therefore, $\zeta \in K(\sqrt[7]{u}) \subseteq \mathbb{R}$. But, this is a contradiction.

(b): We have that $[\Omega : \mathbb{Q}] = 42$. Hence, from (a), we have that $G \cong F_{42}$.

(c): Note that $\mathrm{Gal}(\Omega/K(\sqrt[7]{u}))$ is a subgroup of G of order 2, and hence, there exists H, a subgroup of G of order 6 so that $H \supseteq \mathrm{Gal}(\Omega/K(\sqrt[7]{u}))$ (Hall's Theorem on solvable groups). Let $F = \Omega^H$. Then, $F/\mathbb{Q}$ is an extension of degree 7 so that $F \subseteq K(\sqrt[7]{u})$. If $F/\mathbb{Q}$ were a radical extension, then $F = \mathbb{Q}(\sqrt[7]{a})$ for some $a \in \mathbb{Q}$. Hence, $\mathbb{Q}(\zeta, \sqrt[7]{a}) = \Omega = \mathbb{Q}(\zeta, \sqrt[7]{u})$ and $a = u^i c^7$ for some $c \in \mathbb{Q}(\zeta)$ with $(i, 7) = 1$ (Theorem 2.2). Let N denote the norm of $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$. Taking norm in the previous equation, we have that $a^6 = \pm N(c)^7$, since u is a unit in K and $\mathrm{N}(u) = \pm 1$. Hence, a^6 is a 7th power in $\mathbb{Q}$. But this contradicts the irreducibility of $x^7 - a$ over $\mathbb{Q}$. Therefore, $F/\mathbb{Q}$ is not a radical extension.

(d): We have that $K(\sqrt[7]{u})$ has only two proper subfields: F and K. By Lemma 4.1, K is not contained in a real repeated radical extension. Therefore, $K(\sqrt[7]{u})/\mathbb{Q}$ is not a real repeated radical extension.

(e): Let Ω_1 be the normal closure of F over $\mathbb{Q}$. Assume $[\Omega_1 : \mathbb{Q}] = k$, and let $\alpha \in F$ be so that $F = \mathbb{Q}(\alpha)$. Then, $\Omega_1 \subseteq \mathbb{Q}(\alpha, \zeta) = \Omega$. Since $F/\mathbb{Q}$ is not a Galois extension, we have that $k = 14, 21$ or 42. On the other hand, by Hall's Theorem on solvable groups, all the subgroups of F_{42} of order $42/k$ are conjugates, and by Galois' theory, Ω_1 is the only subfield of the extension $\Omega/\mathbb{Q}$ of degree k over $\mathbb{Q}$. If $k = 14$, then F_{42} would have only one normal subgroup of order 3, contradicting Lemma 4.2. If $k = 21$, then $\Omega_1 = K(\alpha) = K(\sqrt[7]{u})$, again a contradiction, since $K(\sqrt[7]{u})/\mathbb{Q}$ is not a Galois extension. Therefore, the normal closure of $F/\mathbb{Q}$ is Ω.

(f): We shall prove the assertion using Theorem 2.3 as we did in Lemma 4.1. Assume F is contained in a real repeated radical extension. We may assume that $\mathbb{Q} \subseteq L_1 \subseteq L_2 \subseteq \mathbb{R}$ is a tower of fields so that $L_1/\mathbb{Q}$ is a repeated radical extension,

https://doi.org/10.1017/S0004972700019729 Published online by Cambridge University Press

L_2/L_1 is radical, $L_1 \cap F = \mathbb{Q}$ and $F \subseteq L_2$. We shall prove that $L_1 \cap \Omega = \mathbb{Q}$, where $\Omega = \mathbb{Q}(\alpha, \zeta)$ is the normal closure of F over $\mathbb{Q}$ (by (e)). Writing $L = L_1 \cap \Omega(\zeta) = L_1 \cap \Omega$, we have that $L \subseteq \mathbb{R}$, since $L_1 \subseteq \mathbb{R}$. Hence, $L \subseteq L_1 \cap K(\alpha) \subseteq K(\alpha) = K(\sqrt[7]{u})$. By the choice of L_1, we have that $L \neq F, K(\alpha)$, and so the only possibility is $L = \mathbb{Q}$ or $L = K$. By Lemma 4.1, $L \neq K$, and hence $L = \mathbb{Q}$. Therefore, applying Theorem 2.3, $F/\mathbb{Q}$ would be a radical extension, a contradiction. □

THEOREM 4.8. *With the preceding notation, there exists $u \in \mathcal{U}_K \cap \mathbb{R}$ so that*

(i) *$x^7 - u$ is irreducible over $\mathbb{Q}(\zeta)$,*

(ii) *$\Omega/\mathbb{Q}$ is a Galois extension, where $\Omega = \mathbb{Q}(\zeta, \sqrt[7]{u})$ with $\sqrt[7]{u}$ the real root of $x^7 - u$.*

PROOF: We have that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_a \mid \sigma_a(\zeta) = \zeta^a,\ a = 1, \ldots, 6\}$ and $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma_{2|_K} \rangle$. Define

$$u = \prod_{a=1}^{6} \varepsilon^{a^2 \sigma_a^{-1}}, \quad \varepsilon = \zeta^{-1} \frac{1 - \zeta^3}{1 - \zeta}.$$

Then u is a unit in K which is not a 7th power of a unit of K (Theorem 4.6). Let $\Omega = \mathbb{Q}(\zeta, \sqrt[7]{u})$. Then, $\Omega/\mathbb{Q}(\zeta)$ is a cyclic extension of degree 7. This proves (i). For (ii), note that it is easy to see that $\sigma_2(u) = u^4 c^7$ for some $c \in K$. Thus, by Theorem 2.2, $\Omega/\mathbb{Q}$ is a normal extension whose Galois group is the Frobenius group F_{42} of order 42. □

COROLLARY 4.1. *There exists a solvable irreducible polynomial $f(x) \in \mathbb{Q}(x)$ of degree 7 which does not split over $\mathbb{R}$ and the only real root of $f(x)$ does not lie in a real repeated radical extension of $\mathbb{Q}$.*

PROOF: By Theorem 4.8, and keeping the notation as above, we have that there exists $u \in \mathcal{U}_K \cap \mathbb{R}$ which satisfies the hypothesis of Theorem 4.7. Therefore, if $f(x) = \mathrm{irr}(\alpha, \mathbb{Q})$ $\big(F = \mathbb{Q}(\alpha)\big)$, then f is a solvable irreducible polynomial over $\mathbb{Q}$ of degree 7 which does not split over $\mathbb{R}$ (otherwise, $K(\sqrt[7]{u})$ would be the normal closure of F over $\mathbb{Q}$, a contradiction), and f has not a root that lies in a real repeated radical extension of $\mathbb{Q}$ (Theorem 4.7). □

REMARK. The discussion above also provides an example of a number field not contained in a cyclotomic one, where the only finite ramified prime is seven, that is, its discriminant is of the form 7^e for some positive integer e.

REFERENCES

[1] T. Albu and F. Nicolae, 'Kneser field extensions with cogalois correspondence', *J. Number Theory* **52** (1995), 299–318.

[2] F. Barrera-Mora, 'On Subfields of Radical Extensions', *Comm. Algebra* **27** (1999), 4641–4649.

[3] F. Barrera-Mora, M. Rzedowski-Calderón and G. Villa-Salvador, 'On Cogalois extensions', *J. Pure Appl. Algebra* **76** (1991), 1-11.

[4] F. Barrera-Mora and W.Y. Vélez, 'Some results on radical extensions', *J. Algebra* **162** (1993), 295–301.

[5] I.M. Isaacs and D.P. Moulton, 'Real fields and repeated radical extensions', *J. Algebra* **201** (1998), 429–455.

[6] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Maths **83** (Springer-Verlag, New York, Berlin, Heidelberg, 1982).

Departamento de Matemáticas
Escuela Superior de Física y Matemáticas del I.P.N.
Edificio 9 Unidad Profesional ALM, Zacatenco
CP 07300 México, D.F.
México
e-mail: barrera@esfm.ipn.mx
plam@esfm.ipn.mx