JOURNAL OF NUMBER THEORY **60**, 291–309 (1996)
ARTICLE NO. 0124

Finite Radical Field Extensions and Crossed Homomorphisms

Toma Albu*

Facultatea de Matematică, Universitatea Bucureşti,
Str. Academiei 14, RO-70109 Bucureşti 1, Romania

and

Florin Nicolae†

Institutul de Matematică al Academiei Române,
P.O. Box 1-764, RO-70700 Bucureşti 1, Romania

Received January 1995; revised September 18, 1995

We extend to arbitrary finite radical extensions the results of Barrera-Mora and Velez (*J. Algebra* **162** (1993), 295–301) concerning simple radical extensions and we obtain in terms of crossed homomorphisms new characterizations of Kneser extensions and Δ-Cogalois extensions introduced by Albu and Nicolae (*J. Number Theory* **52** (1995), 299–318).

INTRODUCTION

The aim of this paper is twofold: firstly, to extend all the main results of [4], established for simple radical extensions, to arbitrary finite radical extensions, and secondly to provide new characterizations of Kneser extensions and Δ-Cogalois extensions introduced in [1], in terms of crossed homomorphisms.

0. PRELIMINARIES

Throughout this paper F denotes a fixed field, Char(F) its characteristic, and Ω a fixed algebraically closed field containing F as a subfield. Any algebraic extension of F is supposed to be a subfield of Ω.

* E-mail: talbu@roimar.imar.ro.
† E-mail: fnicolae@roimar.imar.ro.

0022-314X/96 $18.00

For an arbitrary nonempty subset S of Ω and a natural number $n \geqslant 1$ we shall use the following notation:

$$S^* = S \setminus \{0\},$$
$$S^n = \{x^n \mid x \in S\},$$
$$\mu_n(S) = \{x \in S \mid x^n = 1\},$$
$$\mu(S) = \{x \in S \mid x^k = 1 \text{ for some } x \in \mathbb{N}^*\}.$$

By a primitive n-th root of unity we mean any generator of the cyclic group $\mu_n(\Omega)$; ζ_n will always denote such an element.

For an arbitrary multiplicative group G the notation $H \leqslant G$ means that H is a subgroup of G. The lattice of all subgroups of G will be denoted by $\underline{\text{Subgroups}}(G)$. For any subset M of G, $\langle M \rangle$ will denote the subgroup of G generated by M. The order of an element $g \in G$ will be denoted by $\text{ord}(g)$. If $G^k = \{e\}$ for some $k \in \mathbb{N}^*$, then the *exponent* $\exp(G)$ of G is the least $n \in \mathbb{N}^*$ such that $G^n = \{e\}$, where e is the identity element of G.

For a field extension E/F we shall denote by $\underline{\text{Subextensions}}(E/F)$ the lattice of all subextensions K/F of E/F, by $[E:F]$ its degree, and if E/F is Galois by $\text{Gal}(E/F)$ its Galois group. For any subgroup H of $\text{Gal}(E/F)$, $\text{Fix}(H)$ will denote the fixed field of H. We shall also use the following notation:

$$T(E/F) = \{x \in E^* \mid x^n \in F^* \text{ for some } n \in \mathbb{N}^*\}.$$

The quotient group $T(E/F)/F^*$ is called in [5] the *Cogalois* group of the extension E/F and is denoted by $\text{Cog}(E/F)$.

For every positive integer $n \geqslant 1$ we shall denote

$$T_n(E/F) = \{x \in E^* \mid x^n \in F^*\} \qquad \text{and} \qquad \text{Cog}_n(E/F) = T_n(E/F)/F^*.$$

If $x \in \Omega^*$, then $\hat{x}$ will denote throughout this paper the coset xF^* in the quotient group Ω^*/F^*.

Let E/F be a field extension with Galois group G and $M \leqslant E^*$ such that $\sigma(M) \subseteq M$ for any $\sigma \in G$. A *crossed homomorphism* or an 1-*cocycle* of G with coefficients in M is a function $f: G \to M$ satisfying the condition: $f(\sigma\tau) = f(\sigma)\,\sigma(f(\tau))$ for all $\sigma, \tau \in G$. The set of all crossed homomorphisms of G with coefficients in M is an abelian group which will be denoted by $Z^1(G, M)$. For any $\alpha \in E^*$ we shall denote by f_α the 1-*coboundary* $f_\alpha: G \to M$ defined as follows: $f_\alpha(\sigma) = \sigma(\alpha) \cdot \alpha^{-1}$, $\sigma \in G$. The set $B^1(G, M) = \{f_\alpha \mid \alpha \in E^*\}$ is a subgroup of $Z^1(G, M)$, and the quotient group $Z^1(G, M)/B^1(G, M)$ is called the first *cohomology group* of G with coefficients in M, and is denoted by $H^1(G, M)$. The famous Hilbert's Theorem 90 asserts that if E/F is a Galois extension, then $H^1(G, E^*) = 1$.

Recall now some definitions from [1]. Let E/F be a field extension; this extension is said to be a *radical* extension if there exists a subset $A \subseteq T(E/F)$ such that $E = F(A)$, or equivalently, if $E = F(T(E/F))$. If $E = F(a)$ for a single element $a \in T(E/F)$, we say that E/F is a *simple radical* extension. The extension E/F is called n-pure for some positive integer n if for any p, $p \mid n$, p odd prime or 4, one has $\mu_p(E) \subseteq F$. Now let Δ be a group. The extension E/F is said to be Δ-*radical* if $F^* \leqslant \Delta \leqslant T(E/F)$ and $E = F(\Delta)$. The extension E/F is said to be Δ-*Kneser* if it is a finite Δ-radical extension such that $|\Delta/F^*| \leqslant [E:F]$, or equivalently, if $|\Delta/F^*| = [E:F]$. The extension E/F is called *Kneser* if it is Δ-Kneser for some group Δ. The class of Kneser extensions include the class of *Cogalois* extensions defined in [5]: the extension E/F is a Cogalois extension if and only if it is $T(E/F)$-Kneser.

Now consider an arbitrary Δ-radical extension E/F. Let

$$\mathscr{E} = \{L \mid F \subseteq L,\ L \text{ subfield of } E\}$$

denote the lattice of all subextensions of the extension E/F, and

$$\mathscr{D} = \{\Gamma/F^* \mid F^* \leqslant \Gamma \leqslant \Delta\},$$

denote the lattice of all subgroups of the quotient group Δ/F^*.

The mappings

$$\varphi\colon \mathscr{E} \to \mathscr{D}, \qquad \varphi(L) = (L \cap \Delta)/F^*,$$

$$\psi\colon \mathscr{D} \to \mathscr{E}, \qquad \psi(\Gamma/F^*) = F(\Gamma)$$

arise in a very natural way, and one can ask: when are φ and ψ isomorphisms of lattices, inverse to one another? We were able to answer this question in [1] for separable Δ-Kneser extensions:

THEOREM 0.1 [1, Theorem 3.7]. *The following assertions are equivalent for a finite separable Δ-radical extension $F \subseteq E$ with Δ/F^* finite and $n = \exp(\Delta/F^*)$:*

(1) *E/F is Δ-Kneser, and the mappings φ and ψ are isomorphisms of lattices, inverse to one another.*

(2) *E/F is n-pure.*

A field extension E/F as in 0.1 is called Δ-*Cogalois*. By [1; Corollary 3.12], the group Δ is uniquely determined, i.e., if E/F is Δ-*Cogalois* an also Γ-*Cogalois*, then necessarily $\Delta = \Gamma$; in this case, the quotient group Δ/F^* will be denoted by $\mathrm{Kne}(E/F)$ and will be called the *Kneser group* of the Δ-Cogalois extension E/F. Note that $\mathrm{Kne}(E/F)$ is a subgroup of $\mathrm{Cog}(E/F)$.

The class of Δ-Cogalois extensions is fairly large, including the classical Kummer extensions, the Kummer extensions with few roots of unity, as well as Cogalois extensions and neat presentations considered in [5] (see [1; Section 5]).

1. GALOIS EXTENSIONS AND CROSSED HOMOMORPHISMS

The aim of this section is to establish a slight modification of a result mainly due to Dummit (see [3; Theorem 7]) giving a nice description of the Cogalois group of a finite Galois extension by means of crossed homomorphisms. Using a result from [2], this provides a description of the Kneser group of a Galois Δ-Cogalois extension in terms of crossed homomorphisms, which extends a result from [5] established for neat presentations.

For a Galois extension E/F consider the following mapping

$$f\colon \mathrm{Gal}(E/F)\times \mathrm{Cog}(E/F)\to \mu(E),$$
$$f(\sigma, \hat{\alpha})=f_{\alpha}(\sigma)=\sigma(\alpha)\cdot\alpha^{-1}.$$

Note that f is well-defined. Clearly, for every integer $n\geqslant 1$, the restriction of f to $\mathrm{Cog}_n(E/F)$ induces a mapping:

$$f_n\colon \mathrm{Gal}(E/F)\times \mathrm{Cog}_n(E/F)\to \mu_n(E).$$

For any fixed $\sigma\in\mathrm{Gal}(E/F)$, the partial mapping $f(\sigma,-)$ is clearly multiplicative on $\mathrm{Cog}(E/F)$, and for any fixed $\hat{\alpha}$, the partial mapping $f(-,\hat{\alpha})$, is precisely the 1-coboundary $f_\alpha\in Z^1(\mathrm{Gal}(E/F),\mu(E))$, so f and f_n induce morphisms of groups

$$\psi\colon \mathrm{Cog}(E/F)\to Z^1(\mathrm{Gal}(E/F),\mu(E)),\qquad \psi(\hat{\alpha})(\sigma)=f(\sigma,\hat{\alpha})$$

and

$$\psi_n\colon \mathrm{Cog}_n(E/F)\to Z^1(\mathrm{Gal}(E/F),\mu_n(E)),\qquad \psi_n(\hat{\alpha})(\sigma)=f_n(\sigma,\hat{\alpha}).$$

PROPOSITION 1.1. *Let E/F be a Galois extension and $n\geqslant 1$ a natural number. Then, the morphism*

$$\psi_n\colon \mathrm{Cog}_n(E/F)\to Z^1(\mathrm{Gal}(E/F),\mu_n(E))$$

defined above is a monomorphism. If E/F is a finite Galois extension, then ψ_n is an isomorphism.

Proof. (1) Denote by G the group $\mathrm{Gal}(E/F)$, and let $\alpha \in T_n(E/F)$. We have

$$\hat{\alpha} \in \mathrm{Ker}(\psi_n) \Leftrightarrow f_\alpha(\sigma) = 1, \ \forall \sigma \in G \Leftrightarrow \sigma(\alpha) = \alpha,$$
$$\forall \sigma \in G \Leftrightarrow \alpha \in \mathrm{Fix}(G) = F,$$

and consequently ψ_n is a monomorphism.

(2) Suppose that E/F is a finite Galois extension. We have to show that ψ_n is surjective. Let $f \in Z^1(G, \mu_n(E))$. Since clearly $f \in Z^1(G, E^*)$, by Hilbert's Theorem 90, there exists $\alpha \in E^*$ such that $f = f_\alpha$. It follows that $\sigma(\alpha)/\alpha \in \mu_n(E)$, so $(\sigma(\alpha)/\alpha)^n = 1$ for every $\sigma \in G$. We deduce that $\sigma(\alpha^n) = \alpha^n$ for every $\sigma \in G$, and consequently $\alpha^n \in F^*$, that is, $\alpha \in T_n(E/F)$. Hence $f = \psi_n(\hat{\alpha})$. ∎

The next result is a special case of [3; Theorem 7].

Corollary 1.2. *Let E/F be a finite Galois extension with Galois group G. Then* $\mathrm{Cog}(E/F) \simeq Z^1(G, \mu(E))$.

Proof. Clearly, for any $n \geqslant 1$, the restriction of the morphism

$$\psi: \mathrm{Cog}(E/F) \to Z^1(\mathrm{Gal}(E/F), \mu(E))$$

to $\mathrm{Cog}_n(E/F)$ is ψ_n. On the other hand, because G is finite, $Z^1(G, \mu(E))$ is the union of all $Z^1(G, \mu_n(E))$, $n \geqslant 1$, and because any ψ_n is surjective by 1.1, we deduce that ψ is surjective. ∎

Remark 1.3. If E/F is an infinite Galois extension then the group $\mathrm{Cog}(E/F)$ is isomorphic to the group of all *continuous* crossed homomorphisms of the compact topological group $\mathrm{Gal}(E/F)$ (endowed with the Krull topology) with coefficients in the discrete group $\mu(E)$, cf. [3; Theorem 7].

Corollary 1.4. *If E/F is a finite Galois extension with Galois group G, then the mapping*

$$\varphi: \{\Delta \mid F^* \leqslant \Delta \leqslant T(E/F)\} \to \{U \mid U \leqslant Z^1(G, \mu(E))\}$$
$$\varphi(\Delta) = \{f_\alpha \in Z^1(G, \mu(E)) \mid \alpha \in \Delta\},$$

is a lattice isomorphism, which induces a canonical lattice isomorphism.

$$\underline{\mathrm{Subgroups}}(\mathrm{Cog}(E/F)) \simeq \underline{\mathrm{Subgroups}}(Z^1(G, \mu(E))).$$

For any cyclic subgroup C of $Z^1(G, \mu(E))$ there exists $\alpha \in T(E/F)$ such that $\varphi(F^*\langle \alpha \rangle) = \langle f_\alpha \rangle = C$. Moreover, if $\varphi(\Delta) = U$, then $\Delta/F^* \simeq U$.

THEOREM 1.5. *Let E/F be a Galois Δ-Cogalois extension with $n = \exp(\Delta/F^*)$. Then*

$$\mathrm{Kne}(E/F) \simeq Z^1(\mathrm{Gal}(E/F), \mu_n(E)).$$

Proof. Denote by G the Galois group of E/F. By 1.1, we have $\mathrm{Cog}_n(E/F) \simeq Z^1(G, \mu_n(E))$. Let $\alpha \in T_n(E/F)$. According to [2; Proposition 3.2], it follows that $\alpha \in \Delta$, so $\Delta = T_n(E/F)$, and consequently

$$\mathrm{Cog}_n(E/F) = T_n(E/F)/F^* = \Delta/F^* = \mathrm{Kne}(E/F). \quad \blacksquare$$

Remark 1.6. As mentioned in the last part of Section 0, the neat presentations are very particular cases of Δ-Cogalois extensions. When E/F is a neat presentation, then Theorem 1.5 gives an intermediate result of [5; p. 267] which has been proved there using a sophisticated technique, including the Lyndon–Hochschild spectral sequence.

For any Galois Δ-Cogalois extension E/F with $n = \exp(\Delta/F^*)$, the mapping

$$f\colon \mathrm{Gal}(E/F) \times \mathrm{Cog}(E/F) \to \mu(E),$$

considered at the beginning of this section yields by restriction the mapping

$$g\colon \mathrm{Gal}(E/F) \times \mathrm{Kne}(E/F) \to \mu_n(E), \qquad g(\sigma, \hat{\alpha}) = f_\alpha(\sigma) = \sigma(\alpha) \cdot \alpha^{-1}.$$

For any $H \leqslant \mathrm{Gal}(E/F)$ and $W \leqslant \mathrm{Kne}(E/F)$ let

$$H^\perp = \{c \in \mathrm{Kne}(E/F) \mid g(\sigma, c) = 1, \forall \sigma \in H\},$$

$$W^\perp = \{\sigma \in \mathrm{Gal}(E/F) \mid g(\sigma, c) = 1, \forall c \in W\}.$$

PROPOSITION 1.7. *For any Galois Δ-Cogalois extension E/F, the assignments $(-)^\perp$ define mutually inverse antiisomorphisms between the lattices* $\underline{\mathrm{Subgroups}}(\mathrm{Gal}(E/F))$ *and* $\underline{\mathrm{Subgroups}}(\mathrm{Kne}(E/F))$.

Proof. For simplicity, denote by G the group $\mathrm{Gal}(E/F)$, by $\mathscr{G}$ the lattice of all subgroups of G, by $\mathscr{D}$ the lattice of all subgroups of $\Delta/F^* = \mathrm{Kne}(E/F)$, and by $\mathscr{E}$ the lattice of all subextensions of the Galois extension E/F.

Because E/F is a Δ-Cogalois extension, the mappings

$$\mathscr{E} \to \mathscr{D}, \qquad L \mapsto (L \cap \Delta)/F^* \qquad \text{and} \qquad \mathscr{D} \to \mathscr{E}, \qquad \Gamma/F^* \mapsto F(\Gamma)$$

are isomorphisms of lattices, inverse to one another, and because E/F is a finite Galois extension, the mappings

$$\mathcal{G} \to \mathcal{E}, \qquad H \mapsto \mathrm{Fix}(H) \qquad \text{and} \qquad \mathcal{E} \to \mathcal{G}, \qquad L \mapsto \mathrm{Gal}(E/L)$$

are antiisomorphisms of lattices, inverse to one another.

If $H \leqslant G$ and $W = \Gamma/F^* \leqslant \Delta/F^*$, where $F^* \leqslant \Gamma \leqslant \Delta$, then it is easily proved that

$$H^\perp = \{\hat{\alpha} \in \Delta/F^* \mid \sigma(\alpha) = \alpha, \forall \sigma \in H\} = (\mathrm{Fix}(H) \cap \Delta)/F^*$$

and

$$W^\perp = \{\sigma \in G \mid \sigma(\gamma) = \gamma, \forall \gamma \in \Gamma\} = \mathrm{Gal}(E/F(\Gamma)).$$

It follows that each of the composed mappings

$$\mathcal{D} \to \mathcal{E} \to \mathcal{G} \qquad \text{and} \qquad \mathcal{G} \to \mathcal{E} \to \mathcal{D}$$

of the canonical bijections considered above gives rise to the mappings $(-)^\perp$ between $\mathcal{D}$ and $\mathcal{G}$, which finishes the proof. ▮

Remark 1.8. If E/F is a Galois Cogalois extension, then Proposition 1.7 gives [5; Theorem 2.2], and if E/F is a neat presentation, then Proposition 1.7 gives an equivalent, but more complete form of [5; Theorem 2.3].

2. RADICAL EXTENSIONS, KNESER EXTENSIONS, COGALOIS EXTENSIONS, AND CROSSED HOMOMORPHISMS

The main purpose of this section is to extend Theorems 2.1, 2.2, 2.3 and 2.4 from [4], established for simple radical extensions, to arbitrary finite radical extensions. Using the setting of crossed homomorphisms, we obtain new characterisations of Kneser and Δ-Cogalois extensions. We will follow in our proofs some of the ideas of [4].

Let E/F be a finite Galois extension with Galois group G. Then, by 1.2, there exists a canonical isomorphism $\mathrm{Cog}(E/F) \simeq Z^1(G, \mu(E))$, hence the canonical mapping

$$f\colon \mathrm{Gal}(E/F) \times \mathrm{Cog}(E/F) \to \mu(E), \qquad f(\sigma, \hat{\alpha}) = \sigma(\alpha) \cdot \alpha^{-1},$$

considered in Section 1 produces, by replacing $\mathrm{Cog}(E/F)$ with its isomorphic copy $Z^1(G, \mu(E))$, precisely the *evaluation mapping*:

$$\langle -, - \rangle\colon G \times Z^1(G, \mu(E)) \to \mu(E), \qquad \langle \sigma, f \rangle = f(\sigma).$$

For any $H \leqslant G$, $U \leqslant Z^1(G, \mu(E))$ and $\chi \in Z^1(G, \mu(E))$ denote

$$H^\perp = \{ f \in Z^1(G, \mu(E)) \mid \langle H, f \rangle = 1 \},$$

$$U^\perp = \{ \sigma \in G \mid \langle \sigma, U \rangle = 1 \}, \qquad \chi^\perp = \{ \sigma \in G \mid \chi(\sigma) = 1 \}.$$

One verifies that $H^\perp$ and $U^\perp$ are again subgroups, and $\chi^\perp = \langle \chi \rangle^\perp$. Note that in the previous section we have also used the notation $(-)^\perp$, but with a different meaning.

THEOREM 2.1. *Let E/F be a finite Galois extension with Galois group G, and K a subfield of E containing F. Then K/F is a radical extension* (*resp. a simple radical extension*) *if and only if there exists $U \leqslant Z^1(G, \mu(E))$* (*resp. $\chi \in Z^1(G, \mu(E))$*) *with* $\mathrm{Gal}(E/K) = U^\perp$ (*resp.* $\mathrm{Gal}(E/K) = \chi^\perp$).

Proof. Suppose that K/F is a radical extension, so there exists $F^* \leqslant \Delta \leqslant T(E/F)$ with Δ/K^* finite and $K = F(\Delta)$. Let $U := \{ f_\alpha \mid \alpha \in \Delta \} \leqslant Z^1(G, \mu(E))$. We have

$$\begin{aligned} U^\perp &= \{ \sigma \in G \mid f_\alpha(\sigma) = 1, \forall \alpha \in \Delta \} = \{ \sigma \in G \mid \sigma(\alpha) = \alpha, \forall \alpha \in \Delta \} \\ &= \{ \sigma \in G \mid \sigma(x) = x, \forall x \in F(\Delta) = K \} = \mathrm{Gal}(E/K). \end{aligned}$$

Conversely, suppose that there exists $U \leqslant Z^1(G, \mu(E))$ with $\mathrm{Gal}(E/K) = U^\perp$. Let $\Delta = \{ \alpha \in E^* \mid f_\alpha \in U \} \leqslant T(E/F)$ be the group of radicals associated to U by 1.4. If $\sigma \in G$, then we have

$$\sigma \in U^\perp \Leftrightarrow f_\alpha(\sigma) = 1, \ \forall \alpha \in \Delta \Leftrightarrow \sigma(\alpha) = \alpha, \ \forall \alpha \in \Delta \Leftrightarrow \sigma(x) = x, \ \forall x \in F(\Delta).$$

It follows that $U^\perp = \mathrm{Gal}(E/F(\Delta))$, and so, $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/F(\Delta))$, hence by Galois Theory we obtain $K = F(\Delta)$, which shows that K/F is a radical extension. The case of simple radical extensions now follows from 1.4. ▌

Remarks 2.2. (1) Theorem 2.1 shows that the study of radical subextensions K/F of E/F is equivalent to the study of subgroups of G which have the form $U^\perp$, for $U \leqslant Z^1(G, \mu(E))$.

(2) For a cyclic subgroup $U = \langle \chi \rangle \leqslant Z^1(G, \mu(E))$ we get [4; Theorem 2.1].

(3) Denote by Radical(E/F) the set of all subextensions K/F of E/F which are radical. With the notation and hypotheses of 2.1, the mapping

$$\underline{\mathrm{Radical}}(E/F) \to \underline{\mathrm{Subgroups}}(Z^1(G, \mu(E))),$$

$$F(\Delta)/F \mapsto \{ f_\alpha \mid \alpha \in \Delta \}, \qquad F^* \leqslant \Delta \leqslant T(E/F),$$

is injective, but in general not surjective. Indeed, if $\{f_\alpha \mid \alpha \in \Delta\} = \{f_\alpha \mid \alpha \in \Delta'\}$, then $\Delta/F^* = \Delta'/F^*$ by 1.4, hence $\Delta = \Delta'$, and so $F(\Delta) = F(\Delta')$, which shows that this mapping is injective.

If we take $F = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta_3)$, then $Z^1(G, \mu(E)) \simeq \mathrm{Cog}(E/F) \simeq \mathbb{Z}_6$ (see e.g. [2; Proposition 2.2(c)]) and $|\underline{\mathrm{Radical}}(E/F)| = 2$, hence the above considered mapping cannot be surjective.

The result below provides characterizations, in terms of crossed homomorphisms, of Kneser and Δ-Cogalois subextensions of finite Galois extensions:

Corollary 2.3. *Let E/F be a finite Galois extension with Galois group G, and let K/F be a finite Δ-radical subextension of E/F, with Δ/F^* a finite group. Denote $U = \{f_\alpha \mid \alpha \in \Delta\} \leqslant Z^1(G, \mu(E))$. Then*:

(1) *The extension K/F is Δ-Kneser iff $(G : U^\perp) = |U|$.*

(2) *Suppose that the extension K/F is Δ-Kneser. Then K/F is Δ-Cogalois if and only if the mapping*

$$\{V \mid V \leqslant U\} \to \{S \mid U^\perp \leqslant S \leqslant G\}, \qquad V \mapsto V^\perp$$

is bijective, or equivalently, an antiisomorphism of lattices.

Proof. (1) The extension K/F is Δ-Kneser if and only if $[K : F] = |\Delta/F^*|$. If we denote $H = \mathrm{Gal}(E/K)$, then $[K : F] = (G : H)$ by Galois Theory, and $\Delta/F^* \simeq U$, so $|\Delta/F^*| = |U|$, by 1.4. On the other hand, $H = U^\perp$ according to 2.1. Summing up, we obtain $[K : F] = |\Delta/F^*|$ if and only if $(G : H) = |U|$ if and only if $(G : U^\perp) = |U|$.

(2) Suppose that the extension K/F is Δ-Kneser. By [1; Theorem 3.7], the extension $K = F(\Delta)$ is Δ-Cogalois if and only if the mapping

$$\{\Gamma \mid F^* \leqslant \Gamma \leqslant \Delta\} \to \{L \mid F \subseteq L,\ L \text{ subfield of } K\}, \qquad \Gamma \mapsto f(\Gamma)$$

is a lattice isomorphism. Since $U \simeq \Delta/F^*$, the lattice $\{\Gamma \mid F^* \leqslant \Gamma \leqslant \Delta\}$ is canonically isomorphic by 1.4 to the lattice $\{V \mid V \leqslant U\}$ via the isomorphism $\Gamma \mapsto V$, where $V \simeq \Gamma/F^*$ is the subgroup of crossed homomorphisms associated to Γ by 1.4. By Galois Theory, the lattices $\{L \mid F \subseteq L,\ L \text{ subfield of } K\}$ and $\{S \mid H \leqslant S \leqslant G\}$ are antiisomorphic via the mapping $L \mapsto S = \mathrm{Gal}(E/L)$. Summing up and using 2.1, we obtain that $K = F(\Delta)$ is Δ-Cogalois if and only if the mapping

$$\{V \mid V \leqslant U\} \to \{S \mid U^\perp \leqslant S \leqslant G\}, \qquad V \mapsto V^\perp$$

is a lattice antiisomorphism. ∎

Let E/F be a finite Galois extension with Galois group G and L/F a finite extension such that $L \cap E = F$. Then, by Galois Theory, the mappings

$$\varepsilon\colon \underline{\text{Subextensions}}(E/F) \to \underline{\text{Subextensions}}(LE/L), \qquad K/F \mapsto LK/L$$

and

$$\lambda\colon \underline{\text{Subextensions}}(LE/L) \to \underline{\text{Subextensions}}(E/F), \qquad K_1/L \mapsto K_1 \cap E/F$$

are isomorphisms of lattices, inverse to one another.

Recall that for any field extension E/F we have denoted by $\underline{\text{Radical}}(E/F)$ the set of all subextensions K/F of E/F which are radical. If now $K/F \in \underline{\text{Radical}}(E/F)$ then there exists a Δ, not necessarily unique, such that $F^* \leqslant \Delta \leqslant T(E/F)$, Δ/F^* is a finite group and $K = F(\Delta)$, hence $LK = L(\Delta_1)$, $L^* \leqslant \Delta_1 \leqslant T(LE/L)$, and $\Delta_1/L \simeq \Delta/F$, where $\Delta_1 = \Delta L^*$. It follows that $\varphi(K/F) \in \underline{\text{Radical}}(LE/L)$, and consequently the restriction of ε to radical extensions gives rise to the injective mapping

$$\rho\colon \underline{\text{Radical}}(E/F) \to \underline{\text{Radical}}(LE/L), \quad F(\Delta)/F \mapsto L(\Delta L^*)/L,$$
$$F^* \leqslant \Delta \leqslant T(E/F),$$

which is not necessarily bijective.

THEOREM 2.4. *Let E/F be a finite Galois extension with Galois group G and L/F a finite extension such that $L \cap E = F$. If $\mu(LE) = \mu(E)$, then the following hold*:

(1) *$\Delta L^* \cap E^* = \Delta$ for any Δ with $F^* \leqslant \Delta \leqslant T(E/F)$.*

(2) *$\Delta_1 = (\Delta_1 \cap E^*)L^*$ for any Δ_1 with $L^* \leqslant \Delta_1 \leqslant T(LE/L)$.*

(3) *The mapping*

$$\rho\colon \underline{\text{Radical}}(E/F) \to \underline{\text{Radical}}(LE/L), \quad F(\Delta)/F \mapsto L(\Delta L^*)/L,$$
$$F^* \leqslant \Delta \leqslant T(E/F)$$

is bijective, and the mapping

$$\underline{\text{Radical}}(LE/L) \to \underline{\text{Radical}}(E/F), \quad L(\Delta_1)/L \mapsto F(\Delta_1 \cap E^*)/F,$$

$$L^* \leqslant \Delta_1 \leqslant T(LE/L)$$

is its inverse.

Proof. (1) The equality is clear.

(2) Denote $G_1 = \mathrm{Gal}(LE/L)$. The mapping

$$G_1 \to G, \qquad \sigma \mapsto \sigma_{|E}$$

is an isomorphism of groups. Since $\mu(LE) = \mu(E)$, this isomorphism induces the group isomorphism:

$$v\colon Z^1(G, \mu(E)) \to Z^1(G_1, \mu(LE)),$$

$$v(f)(\sigma) = f(\sigma_{|E}), \qquad f \in Z^1(G, \mu(E)), \qquad \sigma \in G_1.$$

Let Δ_1 with $L^* \leqslant \Delta_1 \leqslant T(LE/L)$. The inclusion $(\Delta_1 \cap E^*)L^* \subseteq \Delta_1$ is obvious. Now let $\alpha_1 \in \Delta_1$. Then $f_{\alpha_1} \in Z^1(G_1, \mu(LE))$, hence, because the above defined mapping

$$v\colon Z^1(G, \mu(E)) \to Z^1(G_1, \mu(LE)),$$

is an isomorphism, there exists $\alpha \in E^*$ such that $f_{\alpha_1} = v(f_\alpha)$, i.e., $f_{\alpha_1}(\sigma_1) = f_\alpha(\sigma_1\,|_E)$ for all $\sigma_1 \in G_1$. It follows that $\sigma_1(\alpha_1)/\alpha_1 = \sigma_1(\alpha)/\alpha$ for all $\sigma_1 \in G_1$, i.e., $\sigma_1(\alpha_1/\alpha) = \alpha_1/\alpha$ for all $\sigma_1 \in G_1$, hence $\alpha_1/\alpha \in \mathrm{Fix}(\mathrm{Gal}(LE/L)) = L$. We deduce that $\alpha_1 = \alpha y$ for some $y \in L^*$. Thus $\alpha = \alpha_1 y^{-1} \in \Delta_1 \cap E$, which proves the inclusion $\Delta_1 \subseteq (\Delta_1 \cap E^*)L^*$.

(3) To prove that ρ is a surjective mapping, let $K_1/L \in \mathrm{Radical}(LE/L)$. Then $K_1 = L(\Delta_1)$ for some Δ_1 with $L^* \leqslant \Delta_1 \leqslant T(LE/L)$, hence, if we denote $\Delta = \Delta_1 \cap E^*$, we have $F(\Delta) \in \underline{\mathrm{Radical}}(E/F)$, and

$$\begin{aligned}\rho(F(\Delta)) &= L(F(\Delta)) = L(F(\Delta_1 \cap E^*)) = L(\Delta_1 \cap E^*)\\ &= L((\Delta_1 \cap E^*)\, L^*) = L(\Delta_1) = K_1,\end{aligned}$$

which shows that ρ is surjective, hence bijective, and its inverse mapping is that described in the statement of the theorem. ∎

Remark 2.5. (1) If in 2.4 we consider the restriction of ρ to simple radical subextensions of E/F we obtain a more precise form of [4; Theorem 2.2].

(2) The isomorphism v defined in the proof of 2.4 induces the isomorphism of lattices:

$$\{U \mid U \leqslant Z^1(G, \mu(E))\} \to \{U_1 \mid U_1 \leqslant Z^1(G_1, \mu(LE))\}, \qquad (*)$$

$$U \mapsto U_1 = v(U).$$

By 1.4, there exist lattice isomorphisms:

$$\{U \mid U \leqslant Z^1(G, \mu(E))\} \to \{\Delta \mid F^* \leqslant \Delta \leqslant T(E/F)\},$$
$$U \mapsto \Delta = \{\alpha \in E^* \mid f_\alpha \in U\}$$

and

$$\{U_1 \mid U_1 \leqslant Z^1(G_1, \mu(LE))\} \to \{\Delta_1 \mid L^* \leqslant \Delta_1 \leqslant T((LE)/L)\},$$
$$U_1 \mapsto \Delta_1 = \{\alpha_1 \in (LE)^* \mid f_{\alpha_1} \in U_1\}.$$

Now using ($*$) we obtain an isomorphism of lattices:

$$v\colon \{\Delta \mid F^* \leqslant \Delta \leqslant T(E/F)\} \to \{\Delta_1 \mid L^* \leqslant \Delta_1 \leqslant T((LE)/L)\},$$
$$\Delta \mapsto \Delta_1 = \{\alpha_1 \in (LE)^* \mid f_{\alpha_1} \in v(\{f_\alpha \mid \alpha \in \Delta\})\}.$$

We assert that $v(\Delta) = \Delta L^*$ for any Δ with $F^* \leqslant \Delta \leqslant T(E/F)$. Indeed, if $\Delta_1 = v(\Delta)$, then it is easily seen by the above considerations that for an $\alpha_1 \in (LE)^*$ one has

$$\begin{aligned} \alpha_1 \in \Delta_1 &\Leftrightarrow \exists \alpha \in \Delta,\ \forall \sigma_1 \in G_1,\ f_{\alpha_1}(\sigma_1) = f_\alpha(\sigma_1 \mid_E) \\ &\Leftrightarrow \exists \alpha \in \Delta,\ \forall \sigma_1 \in G_1,\ \sigma_1(\alpha_1)/\alpha_1 = \sigma_1(\alpha)/\alpha \\ &\Leftrightarrow \exists \alpha \in \Delta,\ \forall \sigma_1 \in G_1,\ \sigma_1(\alpha_1/\alpha) = \alpha_1/\alpha \\ &\Leftrightarrow \alpha_1/\alpha \in \mathrm{Fix}(\mathrm{Gal}(LE/L)) = L. \end{aligned}$$

Hence $\Delta_1 = v(\Delta) = \Delta L^*$. From 2.4 (1) we deduce that the inverse v^{-1} of v can be described explicitly as follows: $v^{-1}(\Delta_1) = \Delta_1 \cap E^*$, $L^* \leqslant \Delta_1 \leqslant T(LE/L)$.

(3) Another argument for the surjectivity of ρ, due to the referee, is the following one: If $K_1/L \in \underline{\mathrm{Radical}}(LE/L)$, then by 2.1 there exists $U_1 \leqslant Z^1(\mathrm{Gal}(LE/L), \mu(LE))$ so that $\mathrm{Gal}(LE/K_1) = U_1^{\perp}$. Let $v\colon Z^1(G, \mu(E)) \to Z^1(G_1, \mu(LE))$ be the isomorphism considered in the proof of 2.4, and denote $U = v^{-1}(U_1)$. Then it is easily verified that $\mathrm{Gal}(E/K_1 \cap E) = U^{\perp}$. Again by 2.1, we deduce that $K_1 \cap E/F \in \underline{\mathrm{Radical}}(E/F)$, and by Galois Theory we have $\rho(K_1 \cap E/F) = K_1/L$.

Corollary 2.6. *Let E/F be a finite Galois extension and L/F a finite extension such that $L \cap E = F$ and $\mu(LE) = \mu(E)$. Let Δ be such that $F^* \leqslant \Delta \leqslant T(E/F)$, and denote $\Delta_1 = L^*\Delta$. Then*

(1) $|\Delta/F^*| = |\Delta_1/L^*|$ *and* $[F(\Delta) : F] = [L(\Delta_1) : L]$.

(2) *The extension $F(\Delta)/F$ is Δ-Kneser if and only if the extension $L(\Delta_1)/L$ is Δ_1-Kneser.*

(3) *The extension $F(\Delta)/F$ is Δ-Cogalois if and only if the extension $L(\Delta_1)/L$ is Δ_1-Cogalois.*

Proof. (1) Let $U := \{f_\alpha \mid \alpha \in \Delta\}$ be the subgroup of $Z^1(G, \mu(E))$ which corresponds via 2.1 to the radical subextension $F(\Delta)/F$ of the Galois extension E/F, and preserve the notation from the proof of 2.4. If we denote $U_1 = v(U)$, then by 1.4, we have $\Delta/F^* \simeq U$ and $\Delta_1/L^* \simeq U_1$. Since $|U_1| = |U|$ it follows that $|\Delta/F^*| = |\Delta_1/L^*|$. Now, by 2.1, we have

$$[F(\Delta) : F] = (G : U^\perp) = (G_1 : v(U)^\perp) = (G_1 : U_1) = [L(\Delta_1) : L].$$

(2) Following 2.3 (1), the extension $F(\Delta)/F$ is Δ-Kneser if and only if $(G : U^\perp) = |U|$, and similarly, the extension $L(\Delta_1)/L$ is Δ_1-Kneser if and only if $(G_1 : U_1^\perp) = |U_1|$. But $U_1 = v(U)$, so $|U_1| = |U|$, and consequently, by the canonical isomorphism $G_1 \simeq G$, we deduce that $(G_1 : U_1^\perp) = (G : U^\perp)$.

(3) By 2.3 (2), $F(\Delta)/F$ is Δ-Cogalois if and only if it is Δ-Kneser and the mapping

$$\{V \mid V \leqslant U\} \to \{S \mid U^\perp \leqslant S \leqslant G\}, \qquad V \mapsto V^\perp$$

is bijective. Using the canonical isomorphism $G_1 \simeq G$, this condition is equivalent to the fact $L(\Delta_1)/L$ is a Δ_1-Kneser extension and the mapping

$$\{V_1 \mid V_1 = v(V) \leqslant v(U) = U_1\} \to \{S_1 \mid U_1^\perp \leqslant S_1 \leqslant G_1\}, \qquad V_1 \mapsto V_1^\perp$$

is bijective. By 2.3(2), this last condition is equivalent to the fact that $L(\Delta_1)/L$ is Δ_1-Cogalois. ▌

COROLLARY 2.7. *Let E/F be a finite Galois extension and L/F a finite extension such that $L \cap E = F$. Let K be a subfield of E containing F such that LK/L is a Δ_1-radical extension with Δ_1/L^* a finite group of exponent n.*

If $\zeta_n \in E$, then K/F is Δ-radical and $\Delta/F^* \simeq \Delta_1/L^*$, where $\Delta = \Delta_1 \cap E$.

Proof. Using the fact that $L \cap E = F$, we deduce that the restriction mapping to E gives rise to an isomorphism

$$G_1 = \mathrm{Gal}(LE/L) \xrightarrow{\sim} \mathrm{Gal}(E/F) = G.$$

Let $U_1 = \{f_{\alpha_1} \mid \alpha_1 \in \Delta_1\}$ be the subgroup of $Z^1(G_1, \mu(LE))$ which corresponds by 2.1 to the radical subextension $L(\Delta_1)/L$ of the Galois extension LE/L. Since $\alpha_1^n \in L^*$ for any $\alpha_1 \in \Delta_1$, it follows that $f_{\alpha_1}(\sigma_1) \in \mu_n(\Omega)$ for any $\sigma_1 \in G_1$, and consequently $U_1 \leqslant Z^1(G_1, \langle \zeta_n \rangle)$. By 2.1, we have $U_1^\perp = \mathrm{Gal}(LE/L(\Delta_1))$.

As in the proof of Theorem 2.4, the above considered isomorphism

$$G_1 \to G, \sigma \mapsto \sigma_{|E}$$

induces the group isomorphism

$$v\colon Z^1(G, \langle \zeta_n \rangle) \to Z^1(G_1, \langle \zeta_n \rangle),$$
$$v(f)(\sigma) = f(\sigma_{|E}), \quad f \in Z^1(G, \langle \zeta_n \rangle), \quad \sigma \in G_1.$$

Denote $U = v^{-1}(U_1)$. Since $\zeta_n \in E$ one finds $U \leqslant Z^1(G, \mu(E))$. If we denote $\Delta = \{\alpha \in E^* \mid f_\alpha \in U\}$, then, as in 2.5(2), we deduce that $\Delta = \Delta_1 \cap E^*$, $\Delta_1 = \Delta L^*$, and so,

$$L(\Delta_1) \cap E = F(\Delta) = LK \cap E = K.$$

Finally, by the proof of 2.6 (1) we have $\Delta / F^* \simeq \Delta_1 / L^*$. ∎

COROLLARY 2.8. *With the notation and hypotheses from* 2.7, *the extension* K/F *is* Δ-*Kneser* (*resp.* Δ-*Cogalois*) *if and only if* LK/L *is* Δ_1-*Kneser* (*resp.* Δ_1-*Cogalois*).

Proof. Adapt the proof of 2.6. ∎

For the proof of the next theorem we need the following result on algebraic number fields, which is interesting in its own rights.

LEMMA 2.9. *Let* K *be an algebraic number field and* $n \geqslant 2$ *a natural number which has a decomposition* $n = n_1 \cdot \cdots \cdot n_r$, *with* $r \geqslant 1$, $n_1, ..., n_r \geqslant 2$. *Then there exist positive rational integers* $a_1, ..., a_r$ *such that* $a_i^{n_i} \in K^{*n}$, $K^{*n}\langle a_i \rangle / K^{*n} \simeq \mathbb{Z}/n_i\mathbb{Z}$ *for each* $i \in \{1, ..., r\}$, *and*

$$K^{*n}\langle a_1, ..., a_r \rangle / K^{*n} = (K^{*n}\langle a_1 \rangle / K^{*n}) \dot{\times} \cdots \dot{\times} (K^{*n}\langle a_r \rangle / K^{*n})$$

(*internal direct product*), *that is, the numbers* $a_1, ..., a_r$ *are independent modulo* K^{*n}: *for* $k_1, ..., k_r \in \mathbb{N}$ *one has*

$$a_1^{k_1} \cdot \cdots \cdot a_r^{k_r} \in K^{*n} \Leftrightarrow n_i \mid k_i \qquad \textit{for all} \quad i \in \{1, ..., r\}.$$

Proof. Let δ_K be the discriminant of K and $p_1, ..., p_r$ be distinct prime numbers which do not divide δ_K. It follows that $p_1, ..., p_r$ are unramified in K. Denote $a_i := p_i^{n/n_i}$, $i = 1, ..., r$. For every $i \in \{1, ..., r\}$ we choose a prime ideal P_i of the ring of integers of K which lies over p_i and we denote by v_{P_i} the usual P_i-adic valuation on K. Then $v_{P_i}(p_j) = \delta_{ij}$ for every $1 \leqslant i, j \leqslant r$. Clearly, $a_i^{n_i} = p_i^n \in K^{*n}$, $i = 1, ..., r$. Suppose that

$$a_1^{k_1} \cdot \cdots \cdot a_r^{k_r} = x^n \in K^{*n},$$

for some $x \in K^*$. We have

$$n v_{P_i}(x) = v_{P_i}(x^n) = v_{P_i}(a_1^{k_1} \cdot \cdots \cdot a_r^{k_r}) = k_i \frac{n}{n_i},$$

hence $k_i = n_i v_{P_i}(x)$ is a multiple of n_i for each $i \in \{1, ..., r\}$. ∎

In order to state the next theorem we need some preparation. Let K/F be a separable extension of degree n, $L = F(\zeta_n)$ and $E = K(\zeta_n)$. Suppose that:

(1) Char(F) does not divide n,

(2) $K \cap L = F$,

(3) E/L is abelian and E/F is Galois.

Then E/L is an abelian extension of exponent dividing n. By Kummer Theory (see [6; Satz 154, p. 224]), E/L is a Kummer extension, and consequently, by [6; Satz 152, p. 223], there exist $r \geqslant 1, \alpha_1, ..., \alpha_r$ in L^*, and $n_1, ..., n_r \geqslant 2$ such that $n = n_1 \cdot \cdots \cdot n_r$, $E = L(\sqrt[n]{\alpha_1}, ..., \sqrt[n]{\alpha_r})$, $[L(\sqrt[n]{\alpha_i}) : L] = n_i = \text{ord}(\widehat{\sqrt[n]{\alpha_i}})$ for every i, $1 \leqslant i \leqslant r$, $E^{*n} \cap L^* = L^{*n}\langle \alpha_1, ..., \alpha_r \rangle$, $\alpha_1, ..., \alpha_r$ are independent modulo L^{*n}, that is,

$$\alpha_1^{k_1} \cdot \cdots \cdot \alpha_r^{k_r} \in L^{*n} \Leftrightarrow n_i \mid k_i \text{ for every } i \in \{1, ..., r\},$$

and

$$\text{Gal}(E/L) = \langle \tau_1 \rangle \dot{\times} \cdots \dot{\times} \langle \tau_r \rangle,$$

where

$$\tau_i(\sqrt[n]{\alpha_i}) = \zeta_{n_i} \sqrt[n]{\alpha_i} \quad \text{and} \quad \tau_i(\sqrt[n]{\alpha_j}) = \sqrt[n]{\alpha_j} \quad \text{for every} \quad i \neq j, \quad 1 \leqslant i, j \leqslant r.$$

Let $\sigma \in \text{Gal}(L/F)$. We have $\sigma(E^{*n} \cap L^*) \subseteq E^{*n} \cap L^* = L^{*n}\langle \alpha_1, ..., \alpha_r \rangle$. Since $\alpha_i \in E^{*n} \cap L^*$ for every i, $1 \leqslant i \leqslant r$, it follows that there exist uniquely determined elements $\gamma_i^\sigma \in L$ and $0 \leqslant b_{i1}^\sigma < n_1, ..., 0 \leqslant b_{ir}^\sigma < n_r$ such that

$$\sigma(\alpha_i) = (\gamma_i^\sigma)^n \alpha_1^{b_{i1}^\sigma} \cdots \alpha_r^{b_{ir}^\sigma},$$

for all $i \in \{1, ..., r\}$.

Let $n \geqslant 1$ be a natural number. We say that a finite field extension K/F is a *radical extension of exponent dividing n* if there exist a natural number $s \geqslant 1$ and $a_1, ..., a_s \in F^*$ such that $K = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_s})$.

We are now in a position to state the last result of this paper:

THEOREM 2.10. *Let $n \geqslant 2$ be a natural number and K/F a separable extension of degree n. Suppose that the following conditions are satisfied*:

(1) Char(F) *does not divide* n,

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

Then

(a) *If* $K(\zeta_n)/F(\zeta_n)$ *is abelian, then* $K(\zeta_n)/F$ *is Galois.*

(b) K/F *is a radical extension of exponent dividing* n *if and only if* $K(\zeta_n)/F(\zeta_n)$ *is abelian and the following condition is satisfied*:

$$\text{for all } \sigma \in \mathrm{Gal}(F(\zeta_n)/F) \quad \text{and} \quad i, j \in \{1, ..., r\} \quad \text{one has} \quad b_{ij}^{\sigma} = \delta_{ij} \qquad (\dagger)$$

Proof. (a) Apply [4; Proposition 2.5].

(b) Denote $L = F(\zeta_n)$ and $E = K(\zeta_n)$. Suppose that K/F is a radical extension of exponent dividing n. Then, there exists $s \geqslant 1$ and $a_1, ..., a_s \in F^*$ such that $K = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_s})$. We deduce that $E = L(\sqrt[n]{a_1}, ..., \sqrt[n]{a_s})$, E/L is an abelian extension and $E^{*n} \cap L^* = L^{*n}\langle a_1, ..., a_s\rangle$ according to [6; Satz 152, p. 223]. But $E^{*n} \cap L^* = L^{*n}\langle \alpha_1, ..., \alpha_r\rangle$. It follows that $\alpha_i \in L^{*n}\langle a_1, ..., a_s\rangle$, hence $\alpha_i = \theta_i^n c_i$ for some $\theta_i \in L^*$ and $c_i \in \langle a_1, ..., a_s\rangle$, $1 \leqslant i \leqslant s$. Since $\{a_1, ..., a_s\} \subseteq F$, we have $\sigma(c_i) = c_i$, so, if we denote $\gamma_i^{\sigma} = \sigma(\theta_i)/\theta_i \in L$, one obtains

$$\sigma(\alpha_i) = \sigma(\theta_i)^n c_i = \sigma(\theta_i)^n \alpha_i/\theta_i^n = (\sigma(\theta_i)/\theta_i)^n \alpha_i = (\gamma_i^{\sigma})^n \alpha_i$$

for every $\sigma \in \mathrm{Gal}(L/F)$ and $1 \leqslant i \leqslant r$. This shows that $b_{ij}^{\sigma} = \delta_{ij}$ for every $i, j \in \{1, ..., r\}$.

Conversely, suppose that E/L is abelian and the condition $(\dagger)$ is satisfied. Let $\sigma \in H = \mathrm{Gal}(F(\zeta_n)/F)$, so $\sigma(\alpha_i) = (\gamma_i^{\sigma})^n \alpha_i$, $\gamma_i^{\sigma} \in L$, $i = 1, ..., r$. Denote by $\bar{\sigma}$ the unique extension of σ to $E = K(\zeta_n)$ with $\bar{\sigma}_{|K} = 1$, so $\bar{\sigma} \in \bar{H} = \mathrm{Gal}(E/K)$. For any $i \in \{1, ..., r\}$ one has

$$(\bar{\sigma}(\sqrt[n]{\alpha_i}))^n = \bar{\sigma}(\alpha_i) = \sigma(\alpha_i) = (\gamma_i^{\sigma})^n \alpha_i = (\gamma_i^{\sigma} \sqrt[n]{\alpha_i})^n,$$

hence, there exists $\zeta_{i\sigma} \in \langle \zeta_n \rangle$ such that

$$\bar{\sigma}(\sqrt[n]{\alpha_i}) = \gamma_i^{\sigma} \zeta_{i\sigma} \sqrt[n]{\alpha_i} \in L(\sqrt[n]{\alpha_i}).$$

We know that $\mathrm{Gal}(K(\zeta_n)/F(\zeta_n)) = \mathrm{Gal}(E/L) = \langle \tau_1 \rangle \dot{\times} \cdots \dot{\times} \langle \tau_s \rangle$. Therefore $G = \mathrm{Gal}(E/F) = \langle \{\tau_1, ..., \tau_r, \bar{\sigma} \mid \sigma \in H\} \rangle$.

For every $\sigma \in H$ we have clearly $\bar{\sigma}(\zeta_n) = \sigma(\zeta_n) = \zeta_n^{a_\sigma}$, with a_σ and n relatively prime numbers. We claim that

$$\bar{\sigma} \tau_i \bar{\sigma}^{-1} = \tau_i^{a_\sigma}, \qquad i = 1, ..., r.$$

Indeed, for $i \neq j$ we have

$$\bar{\sigma}\tau_i\bar{\sigma}^{-1}(\sqrt[n]{\alpha_j}) = \bar{\sigma}\tau_i(\gamma_j^{\sigma^{-1}}\zeta_{j\sigma^{-1}}\sqrt[n]{\alpha_j}) = \bar{\sigma}(\gamma_j^{\sigma^{-1}}\zeta_{j\sigma^{-1}}\sqrt[n]{\alpha_j})$$
$$= \bar{\sigma}(\bar{\sigma}^{-1}(\sqrt[n]{\alpha_j})) = \sqrt[n]{\alpha_j} = \tau_i^{a_\sigma}(\sqrt[n]{\alpha_j})$$

and

$$\bar{\sigma}\tau_i\bar{\sigma}^{-1}(\sqrt[n]{\alpha_i}) = \bar{\sigma}\tau_i(\gamma_i^{\sigma^{-1}}\zeta_{i\sigma^{-1}}\sqrt[n]{\alpha_i}) = \bar{\sigma}(\gamma_i^{\sigma^{-1}}\zeta_{i\sigma^{-1}}\tau_i(\sqrt[n]{\alpha_i}))$$
$$= \bar{\sigma}(\gamma_i^{\sigma^{-1}}\zeta_{i\sigma^{-1}}\zeta_{n_i}\sqrt[n]{\alpha_i}) = \bar{\sigma}(\bar{\sigma}^{-1}(\sqrt[n]{\alpha_i}))\,\bar{\sigma}(\zeta_{n_i})$$
$$= \sqrt[n]{\alpha_i}\,\zeta_{n_i}^{a_\sigma} = \tau_i^{a_\sigma}(\sqrt[n]{\alpha_i}).$$

Also

$$\bar{\sigma}\tau_i\bar{\sigma}^{-1}(\zeta_n) = \zeta_n = \tau_i^{a_\sigma}(\zeta_n).$$

Consequently

$$G = \langle \{\tau_1, ..., \tau_r, \bar{\sigma} \mid \bar{\sigma} \in \bar{H}, \bar{\sigma}\tau_i\bar{\sigma}^{-1} = \tau_i^{a_\sigma}, \tau_i(\zeta_n) = \zeta_n, \bar{\sigma}(\zeta_n) = \zeta_n^{a_\sigma},$$
$$i = 1, ..., r\} \rangle.$$

We adapt now the idea from the proof of [4; Theorem 2.4], namely to realize the group $G = \mathrm{Gal}(E/F)$ as a Galois group of a suitable radical extension, and then, to apply Theorem 2.1 to conclude that K/F is a radical extension. As known, the Galois group of the Galois extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is isomorphic to the multiplicative group of units of the ring $\mathbb{Z}/n\mathbb{Z}$, and $H = \mathrm{Gal}(F(\zeta_n)/F)$ can be viewed as a subgroup of this Galois group via the embedding $\sigma \mapsto$ congruence class modulo n of a_σ. Denote the F_1 the fixed field of H in $\mathbb{Q}(\zeta_n)$.

If we apply Lemma 2.9 to the algebraic number field $\mathbb{Q}(\zeta_n)$, we find positive rational numbers $a_1, ..., a_r$ with the properties of 2.9. Denote $K_1 = F_1(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$. Then $K_1(\zeta_n) = \mathbb{Q}(\zeta_n)(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$, and therefore $K_1(\zeta_n)/\mathbb{Q}(\zeta_n)$ is a Kummer extension with the Galois group $\langle \rho_1 \rangle \dot{\times} \cdots \dot{\times} \langle \rho_r \rangle$, where

$$\rho_i(\sqrt[n]{a_i}) = \zeta_{n_i}\sqrt[n]{a_i} \qquad \text{and} \qquad \rho_i(\sqrt[n]{a_j}) = \sqrt[n]{a_j}, \qquad 1 \leqslant i \neq j \leqslant r.$$

We claim that the fields $K_1 = F_1(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$ and $\mathbb{Q}(\zeta_n)$ are linearly disjoint over F_1. Indeed, the polynomials $X^{n_i} - a_i \in \mathbb{Q}[X]$, $i = 1, ..., r$ are irreducible over $\mathbb{Q}(\zeta_n)$, hence also over F_1 since F_1 is a subfield of $\mathbb{Q}(\zeta_n)$. But the fields $\mathbb{Q}(\zeta_n)(\sqrt[n]{a_i})$, $i = 1, ..., r$ are linearly disjoint over $\mathbb{Q}(\zeta_n)$. We deduce that the fields $F_1(\sqrt[n]{a_i})$, $i=1, ..., r$ are linearly disjoint over F_1. It follows that

$$\begin{aligned}[F_1(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r}) : F_1] \\ &= [F_1(\sqrt[n]{a_1}) : F_1] \cdot \cdots \cdot [F_1(\sqrt[n]{a_r}) : F_1] \\ &= n_1 \cdot \cdots \cdot n_r = n = [F_1(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r}) \cdot \mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)].\end{aligned}$$

If we denote $\bar{H}_1 = \mathrm{Gal}(K_1(\zeta_n)/K_1)$ and $G_1 = \mathrm{Gal}(K_1(\zeta_n)/F_1)$, then

$$G_1 = \langle \{ \rho_1, ..., \rho_r, \bar{\sigma} \mid \bar{\sigma} \in \bar{H}_1, \bar{\sigma}\rho_i\bar{\sigma}^{-1} = \rho_i^{a_\sigma}, \rho_i(\zeta_n) = \zeta_n, \bar{\sigma}(\zeta_n) = \zeta_n^{a_\sigma}, \\ i = 1, ..., r \} \rangle.$$

Indeed, one has

$$H = \mathrm{Gal}(F(\zeta_n)/F) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/F_1) \simeq \mathrm{Gal}(K_1(\zeta_n)/K_1) = \bar{H}_1,$$

and for any $\bar{\sigma} \in \bar{H}_1$ and $i \in \{1, ..., r\}$ one has $(\bar{\sigma}(\sqrt[n]{a_i}))^n = a_i = (\sqrt[n]{a_i})^n$, and so, $\bar{\sigma}(\sqrt[n]{a_i}) = \zeta_{i\bar{\sigma}} \sqrt[n]{a_i}$ for some $\zeta_{i\bar{\sigma}} \in \langle \zeta_n \rangle$. The relations $\bar{\sigma}\rho_i\bar{\sigma}^{-1} = \rho_i^{a_\sigma}$, $i \in \{1, ..., r\}$ follow now immediately, in a similar way to that used in the proof of the relations $\bar{\sigma}\tau_i\bar{\sigma}^{-1} = \tau_i^{a_\sigma}$.

Moreover, $\langle \tau_i \rangle \simeq \langle \rho_i \rangle \simeq \mathbb{Z}/n_i\mathbb{Z}$ for any $i \in \{1, ..., r\}$, and consequently G and G_1 are isomorphic groups.

Since K_1/F_1 is a radical extension of exponent dividing n, we deduce from Theorem 2.1 that there exists $U_1 \leqslant Z^1(G_1, \langle \zeta_n \rangle)$ with $U_1^\perp = \bar{H}_1$ in G_1. But G and G_1 are isomorphic, and their actions on $\langle \zeta_n \rangle$ are identical, hence the subgroup U_1 can be realized on G as a subgroup $U \leqslant Z^1(G, \langle \zeta_n \rangle)$ with $U^\perp = \bar{H}$ in G, and consequently K/F is a radical extension of exponent dividing n. ∎

ACKNOWLEDGMENTS

The authors are grateful to the referee for valuable comments and suggestions which improved the presentation of the paper. The second author is grateful to the Deutscher Akademischer Austauschdienst for financial support at Berlin during the academic year 1994–1995, when this paper was finished.

REFERENCES

1. T. Albu and F. Nicolae, Kneser field extensions with Cogalois correspondence, *J. Number Theory* **52** (1995), 299–318.
2. T. Albu, F. Nicolae, and M. Ţena, Some remarks on G-Cogalois extensions, *Rev. Roumaine Math. Pures Appl.* **41** (1996), to appear.

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. Velez, Some results on radical extensions, *J. Algebra* **162** (1993), 295–301.
5. C. Greither and D. K. Harrison, A Galois correspondence for radical extensions of fields, *J. Pure Appl. Algebra* **43** (1986), 257–270.
6. H. Hasse, "Vorlesungen über Klassenkörpertheorie," Physica-Verlag, Würzburg/Vienna, 1967.