Turk J Math
26 (2002) , 433 – 445.

Field Extensions Having the Unique Subfield Property, and G-Cogalois Extensions

Toma Albu[*]

Abstract

We present a short proof, based on Cogalois Theory, of a result due to Acosta de Orozco and Vélez (1982, *J. Number Theory* **15**, 388-405) characterizing separable simple radical field extensions with the unique subfield property, and prove that these extensions are precisely the simple G–Cogalois extensions with a cyclic Kneser group.

Key words and phrases: Field extension, separable extension, simple extension, radical extension, G–Cogalois extension, unique subfield property, classical Kummer extension.

Introduction

The aim of this paper is to investigate via Cogalois Theory field extensions with the unique subfield property considered by Vélez [10], [11] and by Acosta de Orozco and Vélez [1]. We present in this framework an alternative proof of the Acosta de Orozco–Vélez Criterion [1] characterizing separable simple radical extensions with the unique subfield property. We show that a separable simple radical extension has the unique subfield property if and only if it is G–Cogalois with cyclic Kneser group. Using this fact, we retrieve immediately a result of Vélez [10].

2000 *Mathematics Subject Classification*: 12E30, 12F05, 12F10, 12F99.

[*]This work was carried out during a stay of the author at the Atilim University, Ankara in the academic year 2001-2002. He would like to thank the University for hospitality and financial support.

0. Preliminaries

Throughout this paper F denotes a fixed field with characteristic exponent $e(F)$ and Ω a fixed algebraic closure of F. Any algebraic extension of F is supposed to be a subfield of Ω.

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

$S^* := S \setminus \{0\}$,

$S^n := \{ x^n \mid x \in S \}$,

$\mu_n(S) := \{ x \in S \mid x^n = 1 \}$.

We denote by $\mathbb{N}$ the set $\{0, 1, 2, \ldots\}$ of all natural numbers, by $\mathbb{N}^*$ the set $\mathbb{N} \setminus \{0\}$ of all strictly positive natural numbers, by $\mathbb{D}_n$ the set of all positive divisors of a given natural number n, by $\mathbb{Z}$ the ring of all rational integers, by $\mathbb{Z}_n$ the ring of all rational integers modulo a positive integer n, and by $\mathbb{Q}$ the field of all rational numbers. If $m, n \in \mathbb{N}$, then $\gcd(m, n)$ will denote the greatest common divisor of m and n. For any set M we denote by $|M|$ the cardinal number of M.

If $x \in \Omega^*$, then $\widehat{x}$ will denote throughout this paper the coset xF^* of x in the quotient group Ω^*/F^*. By a primitive n–th root of unity we mean any generator of the cyclic group $\mu_n(\Omega)$, and ζ_n will always denote such an element.

For an arbitrary multiplicative group G with identity element e, 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. If G is a finite group, then the exponent $\exp(G)$ of G is the least $n \in \mathbb{N}^*$ such that $G^n = \{e\}$. The order of an element $g \in G$ will be denoted by $\mathrm{ord}(g)$.

For a field extension $F \subseteq E$ we shall use the notation E/F, and we shall denote by $[E : F]$ the degree of E/F. Very often, instead of "field extension" we shall use the shorter term "extension". For an extension E/F, the lattice of all intermediate fields K of E/F will be denoted by $\underline{\text{Intermediate}}(E/F)$.

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 [8] the *Cogalois* group of the extension E/F and is denoted by $\mathrm{Cog}(E/F)$.

As in [5], a field extension E/F 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 $E = F(T(E/F))$. A *simple radical* extension is an extension E/F such that there exists an $a \in T(E/F)$ with $E = F(a)$. A field extension E/F is said to be *G–radical* if $F^* \leq G \leq T(E/F)$ and $E = F(G)$.

A basic concept in Cogalois Theory [3] is that of Kneser extension, which has been introduced in [5] as follows: a finite field extension E/F is said to be *G–Kneser* if it is a G–radical extension and $|G/F^*| = [E : F]$. The extension E/F is called *Kneser* if it is G–Kneser for some group G. A finite G–radical field extension E/F is said to be *strongly G–Kneser* if the extension K/F is $K^* \cap G$–Kneser for every intermediate field K of E/F.

The class of finite Kneser extensions includes the class of Cogalois extensions defined in [8]: a finite extension E/F is said to be a *Cogalois* if it is $T(E/F)$–Kneser, that is, if it is radical and $|\mathrm{Cog}\,(E/F)| = [E : F]$. As in [5], a finite field extension is said to be *G–Cogalois* if it is a separable strongly G–Kneser extension. For any G–Cogalois extension E/F, the group G/F^* is uniquely determined; it is called the Kneser group of E/F and denoted by $\mathrm{Kne}(E/F)$.

For any $n \in \mathbb{N}^*$ we denote by $\mathcal{P}_n$ the set of all divisors p of n, with $p \geqslant 3$ a prime number or $p = 4$. As in [8] (resp. [5]) a field extension E/F is said to be *pure* (resp. n–pure, where $n \in \mathbb{N}^*$) if $\mu_p(E) \subseteq F$ for all p, p odd prime or 4 (resp. for all $p \in \mathcal{P}_n$). For all other undefined terms and notation concerning Field Theory the reader is referred to [7] or [9].

For an arbitrary G–radical extension E/F one defines the standard Cogalois connection (see [5])

$$\mathcal{E} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \mathcal{G}$$

between the lattices

$$\mathcal{E} = \underline{\text{Intermediate}}(E/F) = \{ \ K \mid F \subseteq K, \ K \text{ subfield of } E \ \},$$

$$\mathcal{G} = \{ \ H \mid F^* \leqslant H \leqslant G \ \}$$

as follows:

$$\varphi : \mathcal{E} \longrightarrow \mathcal{G}, \ \ \varphi(K) = K \cap G,$$

$$\psi : \mathcal{G} \longrightarrow \mathcal{E}, \ \ \psi(H) = F(H).$$

Observe that $\mathcal{G}$ is canonically isomorphic to the lattice $\underline{\text{Subgroups}}(G/F^*)$ of all subgroups of the group G/F^*.

For the reader's convenience we state below a basic result in Cogalois Theory which will be frequently used throughout this paper.

Theorem 0.1 (Albu and Nicolae [5, Theorem 3.7]). *The following assertions are equivalent for a finite separable G–radical extension E/F with G/F^* finite and $n = \exp(G/F^*)$.*

(1) *E/F is G–Cogalois.*

(2) *E/F is G–Kneser, and the map $\psi : \mathcal{G} \longrightarrow \mathcal{E},\ \psi(H) = F(H)$ is surjective.*

(3) *E/F is G–Kneser, and the maps $-\cap G : \mathcal{E} \longrightarrow \mathcal{G},\ F(-) : \mathcal{G} \longrightarrow \mathcal{E}$ are isomorphisms of lattices, inverse to one another.*

(4) *E/F is n–pure.* □

1. G-Cogalois extensions having the USP

In this section we characterize G–Cogalois extensions having the unique subfield property.

Definition 1.1 (Vélez [10]). *A finite extension E/F is said to have the* unique subfield property*, abbreviated* USP*, if for every divisor m of $[\,E : F\,]$ there exists a unique intermediate field K of E/F such that $[\,K : F\,] = m$.*

Clearly, a finite extension E/F of degree n has the USP if and only if the canonical map

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \mathbb{D}_n,\ K \mapsto [\,K : F\,],$$

is a lattice isomorphism.

Lemma 1.2 *For any irreducible binomial $X^n - a \in F[X]$ and any of its roots $u \in \Omega$, the extension $F(u)/F$ is $F^*\langle u\rangle$–Kneser and $n = \text{ord}(\widehat{u}) = |\,F^*\langle u\rangle/F^*|$.*

Proof. Set $E = F(u)$, $G = F^*\langle u\rangle$, and $k = \exp(G/F^*)$. Clearly, the extension E/F is G–radical, $k = \text{ord}(\widehat{u}) = |G/F^*|$, $k\,|\,n$, and $[\,E : F\,] = n$. We have $u^k = b \in F$, hence $n = [\,F(u) : F\,] \leqslant k$. This implies that $n = k$, i.e.,

$$[\,E : F\,] = |G/F^*|,$$

which shows that E/F is a G–Kneser extension. □

For any finite group A of order n we consider the canonical map

$$\omega_A : \underline{\text{Subgroups}}(A) \longrightarrow \mathbb{D}_n,\ \ B \mapsto |B|.$$

The next result is certainly known (see e.g., Albu and Ion [4]).

Lemma 1.3 *The following assertions are equivalent for a finite group A of order n.*

(1) *A is a cyclic group.*

(2) *The map ω_A is injective.*

(3) *The map ω_A is bijective.*

(4) *The map ω_A is a lattice isomorphism.* □

Proposition 1.4 *The following assertions are equivalent for a finite G–Cogalois extension E/F of degree n.*

(1) *E/F has the* USP.

(2) *The Kneser group G/F^* of E/F is cyclic.*

(3) $G/F^* \cong \mathbb{Z}_n$.

Proof. (1) $\Longrightarrow$ (2): Since the extension E/F is G–Cogalois, the map

$$\underline{\text{Subgroups}}(G/F^*) \longrightarrow \underline{\text{Intermediate}}(E/F),\ H/F^* \mapsto F(H),$$

is a lattice isomorphism by Theorem 0.1.

If the extension E/F has the USP, the map

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \mathbb{D}_n,\ K \mapsto [\,K : F\,],$$

is a lattice isomorphism.

Observe that for any $H/F^* \in \underline{\text{Subgroups}}(G/F^*)$, the extension $F(H)/F$ is H–Kneser by [5, Lemma 3.1], hence $[\,F(H) : F\,] = |H/F^*|$. Consequently, the composition of the two lattice isomorphisms above yields precisely the lattice isomorphism

$$\omega_{G/F^*} : \underline{\text{Subgroups}}(G/F^*) \longrightarrow \mathbb{D}_n,\quad H/F^* \mapsto |H/F^*|.$$

Now, apply Lemma 1.3 to conclude that G/F^* is a cyclic group of order n.

(2) $\Longrightarrow$ (3): Since the extension E/F is in particular G–Kneser, we have

$$n = [\,E : F\,] = |G/F^*|,$$

hence the cyclic group G/F^* is necessarily isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.

(3) $\Longrightarrow$ (1): By Lemma 1.3, the map

$$\omega_{G/F^*} : \underline{\text{Subgroups}}(G/F^*) \longrightarrow \mathbb{D}_n, \;\; H/F^* \mapsto |H/F^*|,$$

is a lattice isomorphism. If we compose it with the lattice isomorphism

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(G/F^*), \; K \mapsto (K \cap G)/F^*,$$

given by Theorem 0.1, we obtain the lattice isomorphism

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \mathbb{D}_n, \; K \mapsto |(K \cap G)/F^*|.$$

Since the extension E/F is G–Cogalois, we have

$$F(K \cap G) = K \;\text{ and }\; |(K \cap G)/F^*| = [\, F(K \cap G) : F\,],$$

hence the composed lattice isomorphism considered above is precisely the map

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \mathbb{D}_n, \; K \mapsto [\, K : F\,].$$

This proves that the extension E/F has the USP. □

Corollary 1.5 *The following assertions are equivalent for a finite Cogalois extension E/F of degree n.*

(1) *E/F has the* USP.

(2) *The Cogalois group* Cog(E/F) *of E/F is cyclic.*

(3) Cog$(E/F) \cong \mathbb{Z}_n$.

Proof. By [5, 5B], the Cogalois extension E/F is $T(E/F)$–Cogalois, and then we have $\text{Kne}(E/F) = T(E/F)/F^* = \text{Cog}(E/F)$. Now apply Proposition 1.4. □

2. The Acosta de Orozco - Vélez Criterion via Cogalois Theory

In this section we present an alternative proof of a result due to Acosta de Orozco and Vélez [1] characterizing separable simple radical extensions with the USP, based on simple facts from Cogalois Theory.

Theorem 2.1 (Acosta de Orozco and Vélez [1, Theorem 2.1]). *Let $u \in \Omega$ be a root of an irreducible binomial $X^n - a \in F[X]$, with $\gcd(n, e(F)) = 1$. The extension $F(u)/F$ has the* USP *if and only if the following two conditions are satisfied.*

(1) $\zeta_p \notin F(u) \setminus F$ for every odd prime divisor p of n.

(2) If $4 \,|\, n$, then $\zeta_4 \notin F(u) \setminus F$.

Proof. Set $E = F(u)$ and $G = F^*\langle u \rangle$. By Lemma 1.2, E/F is a G–Kneser extension, and by [5, Lemma 4.1], the extension E/F is separable.

(1) $\Longrightarrow$ (2): Let $m \in \mathbb{D}_n$. Consider the tower of fields

$$F \subseteq F(u^{n/m}) \subseteq F(u).$$

Since $u^{n/m}$ is a root of the polynomial $X^m - a \in F[X]$, we have $[\,F(u^{n/m}) : F\,] \leqslant m$. A similar argument shows that we also have $[\,F(u) : F(u^{n/m})\,] \leqslant n/m$. On the other hand, by the Tower Law, we have

$$[\,F(u) : F\,] = [\,F(u) : F(u^{n/m})\,] \cdot [\,F(u^{n/m}) : F\,],$$

which implies that

$$[\,F(u^{n/m}) : F\,] = m$$

for any $m \in \mathbb{D}_n$.

Let $K \in \mathcal{E}$. If $m = [\,K : F\,]$, then $m \,|\, n$, and $[\,F(u^{n/m}) : F\,] = m$. Since E/F has the USP, we must have $K = F(u^{n/m})$. Observe that $K = F(H)$, where $H = F^*\langle u^{n/m} \rangle \in \mathcal{G}$, which implies that the map $\psi : \mathcal{G} \longrightarrow \mathcal{E}$, $\psi(H) = F(H)$ is surjective. By Theorem 0.1, we deduce that the G–Kneser extension E/F is actually a G–Cogalois extension, so it is n–pure. Now observe that conditions (1) and (2) mean precisely that the extension E/F is n–pure.

(2) $\Longrightarrow$ (1): As we have already noticed, conditions (1) and (2) say that the extension E/F is n–pure. By Theorem 0.1, E/F is a G–Cogalois extension and the map

$$\underline{\text{Intermediate}}(E/F) \longrightarrow \underline{\text{Subgroups}}(G/F^*),\ K \mapsto (K \cap G)/F^*$$

yields a lattice isomorphism. Since G/F^* is a cyclic group of order n, the map

$$\omega_{G/F^*} : \underline{\text{Subgroups}}(G/F^*) \longrightarrow \mathbb{D}_n, \quad H/F^* \mapsto |H/F^*|$$

is a lattice isomorphism by Lemma 1.3. Now continue as in the proof of Proposition 1.4 to conclude that E/F has the USP. □

3. Simple radical separable extensions having the USP

In this section we investigate simple radical separable extensions having the USP.

Theorem 3.1 *Let* $u \in \Omega$ *be a root of an irreducible binomial* $X^n - a \in F[X]$*, with* $\gcd(n, e(F)) = 1$*. The following assertions are equivalent.*

(1) *The extension* $F(u)/F$ *has the* USP*.*

(2) *The extension* $F(u)/F$ *is* n*–pure.*

(3) *The extension* $F(u)/F$ *is* $F^*\langle u\rangle$*–Cogalois.*

(4) *The extension* $F(u)/F$ *is* G*–Cogalois for some group* G*, and* G/F^* *is a cyclic group.*

Proof. Set $E = F(u)$ and $H = F^*\langle u\rangle$. By Lemma 1.2 we have $\exp(H/F^*) = n$. We have noticed in the proof of Theorem 2.1 that conditions (1) and (2) of Theorem 2.1 mean exactly that E/F is n–pure. So, (1) $\Longleftrightarrow$ (2) by Theorem 2.1, and (2) $\Longleftrightarrow$ (3) by Theorem 0.1.

The implication (3) $\Longrightarrow$ (4) is obvious, while the implication (4) $\Longrightarrow$ (1) follows from Proposition 1.4. □

Remark 3.2 The condition "G/F^* is a cyclic group" in Theorem 3.1 (4) is essential, as the following example shows: Let $F = \mathbb{Q}$, and let $u = \sqrt{2}\,(1+i) \in \mathbb{C}$. Observe that u is a root of the irreducible polynomial $X^4 + 16 \in \mathbb{Q}[X]$. Since $u^2 = 4i$, it follows that $F(u) = \mathbb{Q}(i, \sqrt{2}\,)$. Thus, $F(u)/F$ is a classical 2–Kummer extension, so it is $\mathbb{Q}^*\langle\, i, \sqrt{2}\,\rangle$–Cogalois, but clearly $F(u)/F$ does not have the USP. Observe that $\text{Kne}(F(u)/F) = \mathbb{Q}^*\langle\, i, \sqrt{2}\,\rangle/\mathbb{Q}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is a noncyclic group of order 4. □

The next result shows that, in certain circumstances, the condition "G/F^* is a cyclic group" in point (4) of Theorem 3.1 is superfluous.

Proposition 3.3 *Let* $u \in \Omega$ *be a root of an irreducible binomial* $X^n - a \in F[X]$. *If* $n \not\equiv 0 \pmod 4$ *and* $\gcd(n, e(F)) = 1$, *then the following statements are equivalent.*

(1) *The extension* $F(u)/F$ *has the* USP.

(2) *The extension* $F(u)/F$ *is* $F^*\langle u\rangle$*–Cogalois.*

(3) *The extension* $F(u)/F$ *is* G*–Cogalois for some group* G.

Proof. The proof below is a modified version of a part of the referee's proof for a question raised by the author in the first submitted version of this paper.

Set $E = F(u)$. In view of Theorem 3.1, it is sufficient to prove only that G/F^* is cyclic if E/F is G-Cogalois. Of course we may assume that $n > 2$.

First, we reduce the setup to n a power of a prime number. Let q be a prime divisor of n, and let $n = mq^k$, with m prime to q and $k \geqslant 1$. Set $v = u^m$. One easily checks that $E' = E(v)$ has degree q^k over F, and $X^{q^k} - v^{q^k}$ is an irreducible polynomial over F.

By [6, Proposition 3.1], the extension E'/F is G'-Cogalois for some subgroup G' of G. In particular, E'/F is G'-Kneser, so

$$|G'/F^*| = [\,E' : F\,] = q^k.$$

It follows that G'/F^* is precisely the q-primary component of G/F^*. Since q was an arbitrary prime divisor of n, it will suffice to show that G'/F^* is cyclic. This achieves the reduction, so, without loss of generality, we may assume that $n = p^s$, where p is a prime number and $s \geqslant 2$.

Assume that the group G/F^* is not cyclic, and aim for a contradiction. We cannot have $p = 2$ since, by hypothesis, n is not divisible by 4. Thus, p is an odd prime.

Since $|G/F^*| = [\,E : F\,] = p^s$, it follows that the noncyclic p-group G/F^* has a subgroup U/F^* such that

$$(G/F^*)/(U/F^*) \cong G/U \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

If we denote $K = F(U)$, then, again by [6, Proposition 3.1], the extension E/K is H-Cogalois, where $H = GK^*$. Since $K^* \cap G = F(U) \cap G = U$ by [5, Lemma 3.1], we deduce that

$$H/K^* = (GK^*)/K^* \cong G/(K^* \cap G) = G/U \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Let $x, y \in H$ be such that $H/K^* = \langle \widehat{x}, \widehat{y} \rangle$ and $\langle \widehat{x} \rangle \cap \langle \widehat{y} \rangle = \{\widehat{1}\}$. Then $E = K(x, y)$. We now adjoin ζ_p to both K and E, calling the resulting fields K_1 and E_1, respectively. Since $[\, E : K\,] = |H/K^*| = p^2$ and $[\, K_1 : K\,] \leqslant p-1$, the extensions K_1/K and E/K are linearly disjoint, so $[E_1 : K_1] = p^2$. Now, observe that $E_1 = K_1(x, y)$ and $x^p, y^p \in K \subseteq K_1$, so, the extension E_1/K_1 is H_1-Cogalois by [5, Theorem 5.2], where $H_1 = K_1^*\langle x, y\rangle$. Note that, in fact, E_1/K_1 is a classical p-Kummer extension, and

$$\mathrm{Kne}(E_1/K_1) = H_1/K_1^* \cong \mathrm{Gal}(E_1/K_1) \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

On the other hand, $E_1 = K_1(u)$, and $\exp(K_1^*\langle u\rangle/K_1^*) = \mathrm{ord}(\widehat{u}) = p^k$ for some k with $2 \leqslant k \leqslant s$. Since p is an odd prime, the extension $K_1(u)/K_1$ is clearly p^k-pure, hence it is $K_1^*\langle u\rangle$-Cogalois by Theorem 0.1. But $K_1(u) = E_1$, and we have just seen that the extension E_1/K_1 is H_1-Cogalois. It follows that $H_1 = K_1^*\langle u\rangle$ by the uniqueness of the Kneser group of a G-Cogalois extension (see [5, Corollary 3.12]). This implies that $H_1/K_1^* = K_1^*\langle u\rangle/K_1^*$ is a cyclic group, which is a contradiction. □

Remark 3.4 The "bad" case in Proposition 3.3 appears when n is divisible by 4. By the proof of Proposition 3.3, this is related to whether or not the 2-primary component of the Kneser group of the involved extension E/F is cyclic.

Therefore, we will examine below when a simple radical G-Cogalois extension E/F of degree a power of 2 has a noncyclic Kneser group G/F^*, where F is a field of characteristic $\neq 2$, $E = F(u)$, and u is a root in Ω of an irreducible binomial $X^{2^s} - a \in F[X]$. Since E/F is in particular a G-Kneser extension, we have $|G/F^*| = [\, E : F\,] = 2^s$, and of course $s \geqslant 2$. Then $\exp(G/F^*) = 2^k$ for some $1 \leqslant k \leqslant s$.

If $k \geqslant 2$, then the G-Cogalois extension E/F is 2^k-pure by Theorem 0.1, and hence it is also 2^s-pure. Observe that $\exp(F^*\langle u\rangle/F^*) = \mathrm{ord}(\widehat{u}) = 2^s$ by Lemma 1.2; so, E/F is also $F^*\langle u\rangle$-Cogalois, again by Theorem 0.1. Then, by the uniqueness of the Kneser group of a G-Cogalois extension, we deduce that $G = F^*\langle u\rangle$. This implies that $G/F^* = F^*\langle u\rangle/F^*$ is a cyclic group, which is a contradiction.

Thus, we must have $k = 1$, i.e., $\exp(G/F^*) = 2$, and so, E/F is a classical 2-Kummer extension. Then $E = F(\sqrt{a_1}, \ldots, \sqrt{a_s}\,)$ and

$$G/F^* = F^*\langle\sqrt{a_1}, \ldots, \sqrt{a_s}\,\rangle/F^* \cong (\mathbb{Z}_2)^s,$$

where $\sqrt{a_i}$ denotes a root of a polynomial $X^2 - a_i \in F[X]$ for each $i = 1, \ldots, s$. In particular, E/F is a Galois extension. Since E/F is also $F^*\langle u\rangle$-radical and $\exp(F^*\langle u\rangle/F^*) =$

2^s, it follows that $\zeta_{2^s} \in E$ by [5, Proposition 4.2]. In particular, we have $\zeta_4 = \zeta_{2^s}^{2^{s-2}} \in E$. We cannot have $\zeta_4 \in F$, for otherwise, this would imply that E/F is 2^s-pure, and then as above, it would follow that $G = F^*\langle u\rangle$, which is a contradiction. Thus, without loss of generality, we can choose $a_1 = -1$, and therefore, the given extension E/F is necessarily generated over F by $\zeta_4 = \sqrt{-1}$ and some other square roots $\sqrt{a_2}, \ldots, \sqrt{a_s}$, $s \geqslant 2$, such that $F^*\langle\sqrt{a_1}, \ldots, \sqrt{a_s}\,\rangle/F^* \cong (\mathbb{Z}_2)^s$. In particular, we have $\sqrt{-1} \notin F^*\langle\sqrt{a_2}, \ldots, \sqrt{a_s}\,\rangle$.

It is not clear if any such extension produce an extension we are looking for. However, this happens at least for $s = 2$. More precisely, for any field F of characteristic $\neq 2$ such that $\zeta_4 \notin F$, and for a root $\sqrt{a} \in \Omega$ of any polynomial $X^2 - a \in F[X]$ such that $\sqrt{a} \notin F^*\langle\zeta_4\rangle$, set $E = F(\zeta_4, \sqrt{a}\,)$ and $G = F^*\langle\zeta_4, \sqrt{a}\,\rangle$. Then, the extension E/F is a simple radical quartic G-Cogalois extension with a noncyclic Kneser group of order 4.

Indeed, it is easily checked that the hypotheses about F and $\sqrt{a}$ imply that $E = F(u)$, with $u = (1+\zeta_4)\sqrt{a}$ a root of the polynomial $X^4 + 4a^2 \in F[X]$, which is irreducible by the Vahlen-Capelli Criterion. Notice that the example in Remark 3.2 is a particular case of this more general case. □

Examples 3.5 (1) Any extension of degree a prime number has clearly the USP.

(2) A finite G–radical extension which has USP is not necessarily G–Cogalois. Indeed the extension $\mathbb{Q}(\sqrt{-3}\,)/\mathbb{Q}$ is not $\mathbb{Q}^*\langle\zeta_3\rangle$–Kneser, so it is not $\mathbb{Q}^*\langle\zeta_3\rangle$–Cogalois either.

By [2, Proposition 3.3 and Corollary 5.4], for any square–free integer $d \in \mathbb{N}$, $d \geqslant 2$ and any $n \in \mathbb{Z}^*$ such that $\sqrt{n^2 - d} \notin \mathbb{Q}(\sqrt{d}\,)$, the quartic extension $\mathbb{Q}\left(\sqrt{n + \sqrt{d}}\,\right)/\mathbb{Q}$ has precisely only one quadratic intermediate field, so it has the USP, but is neither a radical nor a Cogalois extension.

Also, any cyclic Galois extension $E/\mathbb{Q}$ of degree > 2 is not G-Cogalois, but has the USP.

(3) A finite G–Cogalois extension may fail to have the USP, as the example in Remark 3.2 shows. Also, a finite Cogalois extension does not have necessarily the USP; e.g., the quartic Cogalois extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)/\mathbb{Q}$ does not have the USP. □

Corollary 3.6 (Vélez [10, Lemma 2.3]). *Let F be an arbitrary field, let $n \in \mathbb{N}^*$ be such that $\gcd(n, e(F)) = 1$, and let $X^n - a$, $X^n - b$ be irreducible polynomials in $F[X]$ with roots $u, v \in \Omega$, respectively. If the extension $F(u)/F$ has the* USP, *then the following assertions are equivalent.*

(1) *The fields $F(u)$ and $F(v)$ are F–isomorphic.*

(2) *There exists* $c \in F$ *and* $j \in \mathbb{N}$ *with* $\gcd(j,n)=1$ *and* $a = b^j c^n$.

Proof. (1) $\Longrightarrow$ (2): If $F(u)$ and $F(v)$ are F–isomorphic, then there exists an F–automorphism σ of Ω such that $F(v) = \sigma(F(u))$. Denote $w = \sigma(u)$. Then $F(v) = F(w)$, and w is a root in Ω of the irreducible polynomial $X^n - a$. Note that the extension $F(v)/F$ also has the USP.

Since $v \in F(w)$, $w^n = a \in F$, and $F(w)/F$ is $F^*\langle w\rangle$–Cogalois by Theorem 3.1, we can apply [2, Lemma 8.4], to deduce that $v \in F^*\langle w\rangle$. Now, observe that since $F(v) = F(w)$, the extension $F(v)/F$ is $F^*\langle v\rangle$–Cogalois again by Theorem 3.1, hence $w \in F^*\langle v\rangle$ using a similar argument. Thus, we have $F^*\langle v\rangle = F^*\langle w\rangle$, and then $w = cv^j$ for some $c \in F^*$ and $j \in \mathbb{N}^*$. Raising this last equation to the n-th power we obtain $a = b^j c^n$. Since $\operatorname{ord}(\widehat{v}) = \operatorname{ord}(\widehat{w}) = n$, it follows that j and n are relatively prime numbers.

(2) $\Longrightarrow$ (1): We can write the equation $a = b^j c^n$ as $u^n = (cv^j)^n$, hence $cv^j = \zeta u$ for some $\zeta \in \mu_n(\Omega)$. If we denote $w = \zeta u$, then w is a root of the irreducible polynomial $X^n - a \in F[X]$, so w is a conjugate of u over F. Now, observe that the equation $cv^j = w$, with $c \in F^*$ and $\gcd(j,n) = 1$ implies that $F^*\langle v\rangle = F^*\langle w\rangle$. Then $F(v) = F(w)$, so $F(u)$ and $F(v)$ are conjugate over F. □

Corollary 3.7 *Let* F *be an arbitrary field, and let* $n \in \mathbb{N}^*$ *be such that* $\zeta_n \in F$ *and* $\gcd(n, e(F)) = 1$. *Let* $X^n - a$, $X^n - b$ *be irreducible polynomials in* $F[X]$ *with roots* u, $v \in \Omega$, *respectively. Then, the following assertions are equivalent.*

(1) $F(u) = F(v)$.

(2) *There exists* $c \in F$ *and* $j \in \mathbb{N}$ *with* $\gcd(j,n)=1$ *and* $a = b^j c^n$.

Proof. Since $\zeta_n \in F$, the extension $F(u)/F$, is a classical n–Kummer extension, so it is $F^*\langle u\rangle$–Cogalois by [5, Theorem 5.2], and by Theorem 3.1, it has the USP. Now observe that the fields $F(u)$ and $F(v)$ are F–isomorphic if and only if they coincide. Apply Corollary 3.6 to deduce the desired result. □

Acknowledgements

The author is indebted to the referee for valuable comments and suggestions, and especially for partially answering an open question raised in the first submitted version of this paper (see Proposition 3.3).

References

[1] Acosta de Orozco, M., Vélez, W.Y.: *The lattice of subfields of a radical extension*. J. Number Theory **15**, 388-405 (1982).

[2] Albu, T.: *Some examples in Cogalois Theory with applications to elementary Field Arithmetic*. J. Algebra Appl. **1**, 1-29 (2002).

[3] Albu, T.: *Cogalois Theory*. New York. A Series of Monographs and Textbooks, Marcel Dekker, Inc. 2002.

[4] Albu, T., Ion, I.D.: *An Elementary Itinerary in Higher Algebra* (in Romanian). Bucureşti. All Educational 1997.

[5] Albu, T., Nicolae, F.: *Kneser field extensions with Cogalois correspondence*. J. Number Theory **52**, 299-318 (1995).

[6] Albu, T., Nicolae, F., Ţena, M.: *Some remarks on G-Cogalois field extensions*. Rev. Roumaine Math. Pures Appl. **41**, 145-153 (1996).

[7] Bourbaki, N.: *Algèbre*, Chapitres 4 à 7. Paris. Masson 1981.

[8] Greither, C., Harrison, D.K.: *A Galois correspondence for radical extensions of fields*. J. Pure Appl. Algebra **43**, 257-270 (1986).

[9] Karpilovsky, G.: *Topics in Field Theory*. Amsterdam New York Oxford Tokyo. North-Holland 1989.

[10] Vélez, W.Y.: *On normal binomials*. Acta Arith. **36**, 113-124 (1980).

[11] Vélez, W.Y.: *Several results on radical extensions*. Arch. Math. (Basel) **45**, 342-349 (1985).

Toma ALBU
Atilim University
Department of Mathematics
06836 İncek, Ankara-TURKEY
e-mail: albu@atilim.edu.tr

Received 28.02.2002