An. Şt. Univ. Ovidius Constanţa Vol. 10(1), 2002, 149–160

# EXTENSIONS HAVING REDUCED SUBEXTENSIONS

**Aurelian Claudiu Volf**

**Abstract**

The concepts of reduced subextension and primitive subextension of a field extension, recently introduced in connection with fuzzy Galois theory, are investigated. We prove that every extension having a proper reduced subextension is algebraic (it was known that its transcendence degree is at most 1). The notion of reduced subgroup of a group is introduced as a natural group theoretic counterpart of the concept of reduced subextension. We determine all finite groups posessing a reduced subgroup. Consequently, the finite Galois and $G$-Cogalois extensions having a reduced intermediate field are determined. We also investigate some properties of the primitive extensions.

## 1 Reduced subextensions

Let $F/K$ be a field extension and let $\mathcal{I}(F/K) = \{L \mid L$ subfield of $F, K \subseteq L\}$ be the lattice of its intermediate fields (also called its subextensions). If $F/K$ is a field extension and $c \in F$ is algebraic over $K$, then we denote by $\mathrm{Irr}(c, K) \in K[X]$ the minimal polynomial of $c$ over $K$. We write $A \subset B$ for $A \subseteq B$ and $A \neq B$.

**1.1. Definition.** [2] Let $L \in \mathcal{I}(F/K)$. Then $L$ is said to be reduced in $F$ over $K$ if $L \neq F$ and $\forall c, d \in F \setminus L$, $L(c) = L(d)$ implies $K(c) = K(d)$.

**1.2 Theorem.** ([2], Th. 1.2) *Let $L \in \mathcal{I}(F/K)$. Then $L$ is reduced in $F$ over $K$ if and only if $F \neq L$ and $\forall c \in F \setminus L$, $L \subseteq K(c)$.*

**Proof.** Suppose that $L$ is reduced in $F$ over $K$. Let $c \in F \setminus L$ and let $b \in L$. Then $L(c) = L(b+c)$ and so $K(c) = K(b+c)$. Hence $b \in K(c)$. Thus $L \subseteq K(c)$.

Key Words: Field extension, algebraic, Galois, Cogalois, lattice of subgroups.
Mathematical Reviews subject classification: 12F05, 12F20, 20D30.

Conversely, suppose that $L \neq F$ and $\forall c \in F\ L$, $L \subseteq K(c)$. Let $c, d \in F \setminus L$. Then $K(c) = L(c)$ and $K(d) = L(d)$. Hence $L(c) = L(d)$ implies that $K(c) = K(d)$. Thus $L$ is reduced in $F$ over $K$. □

Here is a simpler characterization of the reduced subextensions of $F/K$, in terms of the lattice $\mathcal{I}(F/K)$.

**1.3 Theorem.** *Let $L \in \mathcal{I}(F/K)$, $L \neq F$. Then $L$ is reduced in $F$ over $K$ if and only if, $\forall M \in \mathcal{I}(F/K)$, $M \subseteq L$ or $L \subseteq M$.*

**Proof.** "$\Rightarrow$" Let $M \in \mathcal{I}(F/K)$ with $M \not\subseteq L$. Then $\exists c \in M \setminus L$. By the proposition above, $L \subseteq K(c)$; since $K(c) \subseteq M$, $L \subseteq M$.
"$\Leftarrow$" Let $c \in F \setminus L$. Then $K(c) \not\subseteq L$, so $L \subseteq K(c)$. □

So, if $L$ is reduced in $F$ over $K$, $\mathcal{I}(F/K) = I(F/L) \cup I(L/K)$. This is quite a strong condition on the lattice $\mathcal{I}(F/K)$. The following two consequences are immediate from this characterization:

**1.4 Corollary.** *The extension $F/K$ has the property that every $L \in \mathcal{I}(F/K)$ with $L \neq F$ is reduced in $F$ over $K$ if and only if $\mathcal{I}(F/K)$ is a chain (i.e., totally ordered with respect to inclusion).* □

**1.5 Corollary.** *Let $K \subseteq E \subseteq L \subseteq J \subseteq F$ be a chain of field extensions. If $L$ is reduced in $F$ over $K$, then $L$ is reduced in $J$ over $E$.* □

Let $F/K$ be an extension possessing a reduced intermediate field $L \neq K$. Theorem 1.5 in [2] states that $\operatorname{trdeg}(F/K) \leq 1$, where trdeg denotes the transcendence degree. Also, Theorem 1.9 in [2] affirms that $F/K$ is algebraic, provided $\operatorname{char} K = p > 0$ and either $L/K$ is algebraic or $L = K(F^{p^e})$ for some positive integer $e$. It turns out that $F/K$ *is always algebraic:*

**1.6 Theorem.** *Let $F/K$ be an extension possessing a reduced intermediate field $L \neq K$. Then $F/K$ is algebraic.*

**Proof.** First, we prove that $F/L$ is algebraic. Let $y \in F \setminus L$. If $y$ is transcendental over $K$, then $K \subset L \subset K(y)$ since $L$ is reduced in $F/K$. By Lüroth's theorem, $y$ is algebraic over $L$ and $L = K(x)$ for some $x \in L$, transcendental over $K$. If $y$ is algebraic over $K$, it is also algebraic over $L$. So, anyway, $y$ is algebraic over $L$. It is now enough to prove that $L/K$ is algebraic. Suppose that $L/K$ *is not algebraic.* If $y \in F \setminus L$, $y$ is transcendental over $K$. Indeed, we have $K \subset L \subset K(y)$; $y$ algebraic over $K$ would imply $L/K$ algebraic, contradiction. So every $y \in F \setminus L$ is transcendental over $K$ and the argument above shows that $L = K(x)$ for some $x \in F$, transcendental over $K$, and $F/L$ is algebraic. Pick $y \in F \setminus L$. We have therefore the situation: $K \subset K(x) \subset K(y)$, $x$ transcendental over $K$, $K(x)$ reduced in $K(y)$ and $y$ algebraic over $K(x)$. Considering $K(xy)$, we have either $K(xy) \subseteq K(x)$ (but then $y \in K(x)$, contradiction), or $K(x) \subseteq K(xy)$, so $x \in K(xy) \Rightarrow y \in K(xy) \Rightarrow K(y) = K(xy)$. Thus, $K \subset K(x) \subset K(y) = K(xy)$.

We use the following elementary result: *If* $K \subseteq K(t)$ *is a simple transcendental extension and* $z = f(t)/g(t) \in K(t)$, *where* $f, g \in K[T]$, $\gcd(f, g) = 1$, $f(t)g(t) \neq 0$, *then* $\mathrm{Irr}(t, K(z)) = f(T) - zg(T) \in K(z)[T]$ *and* $[K(t) : K(z)] = \deg(f(T) - zg(T)) = \max(\deg f, \deg g)$. [See for instance [5], Ex.1.17.]

Since $x \in K(y)$, there exist univariate nonzero polynomials $a\alpha, \beta \in K[T]$ (where $T$ is an indeterminate) such that:

$$s = \alpha(y)/\beta(y), \gcd(\alpha, \beta) = 1,\ \alpha\beta \neq 0. \tag{$*$}$$

Then $\mathrm{Irr}(y, K(x)) = \beta(T) - x\alpha(T) \in K(x)[T]$. Also, $K(x) \subset K(y)$ implies:

$$\deg \mathrm{Irr}(y, K(x)) = [K(y) : K(x)] = \max(\deg \alpha, \deg \beta) \geq 2.$$

We have $y \in K(xy)$, so there exist nonzero $u, v \in K[T]$ such that:

$$y = u(xy)/v(xy), \gcd(u, v) = 1, uv \neq 0.$$

Since $K(xy) = K(y)$ and $\mathrm{Irr}(xy, K(y)) = u(T) - yv(T)$ has degree $\max(\deg u, \deg v)$, equal to $[K(xy) : K(y)] = 1$, we have $\max(\deg u, \deg v) = 1$. Using $(*)$, we obtain:

$$y \cdot v(y\alpha(y)/\beta(y)) = u(y\alpha(y)/\beta(y))$$

Since $y$ is transcendental over $K$, we have the equality in $K(T)$ :

$$T \cdot v(T\alpha(T)/\beta(T)) = u(T\alpha(T)/\beta(T)) \tag{$**$}$$

Setting $T = 0$ in $(**)$, we get $u(0) = 0$, so $u = T \cdot u'$, with $u' \in K[T]$. But $\deg u \leq 1$, so we may suppose $u = T$. Simplifying in $(**)$, and putting $v(T) = cT + d$, with $c, d \in K$, we have

$$cT\alpha(T) + d\beta(T) = \alpha(T) \tag{$***$}$$

We get $d\beta(T) = \alpha(T)(1 - cT)$, so $\alpha$ divides $d\beta$ in $K[T]$. But $\gcd(\alpha, \beta) = 1$, so $\alpha$ divides $d$, which means $\deg \alpha = 0$. We may as well suppose $\alpha = 1$, so $d\beta(T) = 1 - cT$, which implies $\deg \beta = 1$. This contradicts $\max(\deg \alpha, \deg \beta) \geq 2$ and shows that $F/K$ must be algebraic. $\square$

Let $F/K$ be a finite Galois extension with Galois group $G$. Since there exists an order reversing bijection between $\mathcal{I}(F/K)$ and the lattice of the subgroups of $G$, the following definition appears natural:

**1.7 Definition.** Let $(G, \cdot)$ be a group and 1 its neutral element. Let $\mathcal{S}(G) = \{H \mid H \leq G\}$ be the lattice of subgroups of $G$. We call a subgroup $R \leq G$ *reduced in* $G$ if $R \neq 1$, $R \neq G$ and if $\forall H$, $H \leq G$ implies $H \leq R$ or $R \leq H$. If $S \subseteq G$, let $< S >$ denote the subgroup generated by $S$. For any set $A$, $|A|$ denotes the cardinal of $A$.

So, *a finite Galois extension $F/K$ has a reduced intermediate field $L \neq K$ if and only if* $\mathrm{Gal}(F/K)$ *has a reduced subgroup.* We determine now all finite groups having reduced subgroups.

**1.8 Theorem.** *Let $G$ be a finite group. There exists a reduced subgroup $R$ in $G$ if and only if $G$ is of one of the following types:*

i) *$G$ is cyclic of order $p^n$ (where $p$ is a prime number and $n \in \mathbb{N}^*$). In this case $\mathcal{S}(G)$ is a chain (hence every proper subgroup of $G$ is reduced).*

ii) *$G$ is isomorphic to a generalized quaternion group of order $2^n$ $(n \geq 3)$ : $G =< a, b >$, with $a^{2^{n-1}} = 1$, $b^2 = a^{2^{n-2}}$, $ba = a^{-1}b$. In this case $R$ is the unique minimal proper subgroup of $G$ and $|R| = 2$.*

Before proceeding to the proof we collect some useful results.

**1.9 Proposition.** *Let $G$ be a group and $R \leq G$, $R \neq G$, $R \neq 1$. Then $R$ is a reduced subgroup of $G$ if and only if for every $x \in G \setminus R$, $R \subset< x >$ .*

**Proof.** If $R$ is reduced and $x \in G \setminus R$, then $< x >$ cannot be included in $R$, so $R \subset< x >$ .

Conversely, suppose $R$ has the property that $R \subset< x >$ for every $x \in G \setminus R$. Let $H \in \mathcal{S}(G)$. If $H \subseteq R$, we are done; else there exists $x \in H \setminus R$ and so $R \subset< x >\subseteq H$. $\square$

**1.10 Proposition.** *Let $G$ be a finite group. Then:*

a) *If $R$ is a reduced subgroup of $G$, then $R$ is a characteristic subgroup of $G$ (hence $R$ is normal in $G$).*

b) *If $R$ is a reduced subgroup of $G$ and $H$ is a reduced subgroup of $R$, then $H$ is a reduced subgroup of $G$.*

c) *$\mathcal{S}(G)$ is a chain if and only if $G$ is a cyclic $p$-group for some prime $p$.*

d) *If $G$ is abelian and has a reduced subgroup then $G$ is a cyclic $p$-group (so $\mathcal{S}(G)$ is a chain).*

**Proof.** a) If $\varphi$ is an automorphism of $G$, then $|\varphi(R)| = |R|$. Since $R \subseteq \varphi(R)$ or $\varphi(R) \subseteq R$, we have $R = \varphi(R)$.

b) Let $J \leq G$. If $J$ includes $R$, then $J$ includes $H$ and we are done. If $R$ does not include $R$, then $J \leq R$ since $R$ is reduced. So $J \leq H$ or $H \leq J$ since $H$ is reduced in $R$. We remark that the statement is true for any group $G$.

c) If $G$ is cyclic of order $p^n$, with $p$ prime, then $\mathcal{S}(G)$ is clearly a chain. Suppose now that $\mathcal{S}(G)$ is a chain and let $p$ be a prime divisor of $|G|$. If $|G|$ has another prime divisor $q$, then by Cauchy's Theorem there exist $x, y \in G$ with $\operatorname{ord} x = p$ and $\operatorname{ord} y = q$. Then $< x > \not\subseteq > y >$ and $< y > \not\subseteq < x >$, contradiction. So $|G| = p^n$ for some $n \in \mathbb{N}$. We prove that $G$ is cyclic. This is obvious for $n = 1$. Suppose now that $n > 1$. Then $G$ has a subgroup $H$ of order $p^{n-1}$ ([4], Satz 7.2e)). If $x \in G \setminus H$, then $< x >$ is not included in $H$, so $H \subset < x >$ and so $< x >= G$.

d) Because $G$ is finite abelian, $G$ is cyclic or a direct product of at least two cyclic subgroups. If $G$ is the direct product of its proper subgroups $G_1$ and $G_2$, then $G$ cannot have a reduced subgroup $R$. Indeed, if $R \subseteq G_1$ and $R \subseteq G_2$ then $R \subseteq G_1 \cap G_2 = 1$; if $G_1 \subseteq R$ and $R \subseteq G_2$ then $G_1 \subseteq G_2$; if $G_1 \subseteq R$ and $G_2 \subseteq R$ then $G = G_1 G_2 \subseteq R$. None of these conclusions is consistent with the hypotheses. So $G$ is cyclic and, by the argument above, it cannot be written as a direct product of proper subgroups. This means that $G$ is cyclic of order a power of a prime. $\square$

**Proof** of the Theorem 1.8. Assume that $R$ is a reduced subgroup of $G$. We show first that $R$ is a cyclic $p$-group (hence $\mathcal{S}(R)$ is a chain). Since $R \neq G$ and $G$ is finite, there exists $H \leq G$ with $R < H$ and $H$ is minimal including $R$ (there are no subgroups between $R$ and $H$). Then $R$ is reduced in $H$ (so $H \lhd R$) and $H/R$ has no proper subgroups. So $H/R$ is cyclic of prime order $p$. If $x \in H \setminus R$, then $< x >$ must include $R$, so $< x >= H$. Thus, $H$ is cyclic and has a reduced subgroup. By d), $H$ is a cyclic $p$-group and $\mathcal{S}(H)$ is a chain. So $R$ is also a cyclic $p$-group and $\mathcal{S}(R)$ is a chain.

If $q$ is a prime divisor of $|G|$, then there exists $x \in G$, $\operatorname{ord} x = q$. If $q \neq p$, then $< x > \subseteq R$ implies $\operatorname{ord} x$ is a power of $p$, contradiction; $R \subseteq < x >$ implies $|R| = q$, contradiction. So $|G|$ has only one prime divisor, namely $p$.

We have shown that $G$ is a $p$-group. $G$ has only one subgroup with $p$ elements (the unique subgroup of $R$ with $p$ elements). Indeed, if $J \leq R$ has $p$ elements, then $J \subseteq R$ (for $R \subset J$ would imply $R = 1$, absurd) and $\mathcal{S}(R)$ is a chain, so it contains at most one subgroup of order $p$.

The claim of the theorem follows now from:

**Theorem** ([3], THEOREM 12.5.2, p. 189). *A $p$-group which contains only one subgroup of order $p$ is cyclic or a generalized quaternion group.*

The case of a cyclic $p$-group is clear.

Suppose that $G$ is a generalized quaternion group of order $2^n$ $(n \geq 3)$. It is easy to see that $R =< a^{2^{n-2}} >=< b^2 >$ has 2 elements and is included in every proper subgroup of $G$. Also, $R$ is the only reduced subgroup of $G$. $\square$

Theorem 1.8 and the Galois correspondence yield the following *classification of the extensions having a non-trivial reduced subextension:*

**1.11 Theorem.** *Let $F/K$ be a finite Galois extension with Galois group $G$. Then there exists $L \in \mathcal{I}(F/K)$, $K \neq L \neq F$, such that $L$ is reduced in $F$ over $K$, if and only if $G$ is of one of the following types:*

a) *$G$ is cyclic of order $p^n$ (where $p$ is a prime number and $n \in \mathbb{N}^*$). In this case $\mathcal{I}(F/K)$ is a chain (hence every proper intermediate extension is reduced in $F$ over $K$).*

b) *$G$ is isomorphic to a generalized quaternion group of order $2^n$ $(n \geq 3)$. In this case $L$ is the unique maximal proper intermediate field of $F/K$ and $[F : L] = 2$.* $\square$

**1.12 Remarks.** a) Any extension $F/K$ of finite fields is Galois and the Galois group is cyclic. So $F/K$ has a proper intermediate field reduced in $F$ over $K$ $\Leftrightarrow$ the degree $[F : K]$ is a power of a prime $\Leftrightarrow$ $\mathcal{I}(F/K)$ is a chain $\Leftrightarrow$ every intermediate field of $F/K$ is reduced.

b) A famous result of Šafarevič [8] implies that for every finite solvable group $G$ there exists a finite Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $G$. This ensures that for every type of extension described in Theorem 1.11 there exists an extension of $\mathbb{Q}$ of that type. In particular, there exists a Galois extension $F/\mathbb{Q}$ of degree 8, with Galois group the quaternion group. This extension admits a reduced intermediate field, but $\mathcal{I}(F/\mathbb{Q})$ is not a chain. This is a "minimal" example of extension having a proper reduced intermediate field, but whose intermediate fields are not chained.

c) Let $F/K$ be a separable finite extension and let $N$ be the normal closure of $F/K$. Let $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(N/F)$. The lattice $\mathcal{I}(F/K)$ is antiisomorphic to the lattice of the subgroups of $G$ that include $H$. Thus, the problem of determining the separable finite extensions having a proper reduced intermediate field is translated via Galois theory into the following group theoretical problem:

*Determine all pairs $(G, H)$, where $G$ is a finite group and $H \leq G$, such that there exists a subgroup $R$, $H < R < G$ with the property: for any subgroup $J$, $H \leq J \leq G$ implies $J \leq R$ or $R \leq J$.*

There is another type of extensions $F/K$ for which a bijective correspondence between $\mathcal{I}(F/K)$ and the subgroups of a certain group is available, namely the $G$-Cogalois extensions. Consequently, we obtain a description of the $G$-Cogalois extensions possessing a reduced subextension. We briefly state the definitions and the results we need from [1], where a detailed account of the theory is given.

If $F$ is a field, then $F^*$ denotes the multiplicative group of the nonzero elements of $F$. We suppose all algebraic extensions of $F$ are subfields of $\Omega$, an algebraic closure of $F$. For any field extension $F/K$, define the subgroup of $F^*$:

$$T(F/K) = \{x \in F^* \mid \exists n \geq 1 \text{ with } x^n \in K^*\}.$$

**1.13 Definition.** Let $F/K$ be a field extension. Let $G$ be a group, $K^* \leq G \leq T(F/K)$. The extension $F/K$ is called:

– *$G$-radical* if $F = K(G)$.

– *$G$-Kneser* if it is finite, $G$-radical and $|G/K^*| \leq [F : K]$.

[[1], Prop. 2.4] says: *If $F/K$ is finite and $G$-radical, then: $F/K$ is $G$-Kneser $\Leftrightarrow$ $|G/K^*| = [F : K]$ (there exists a set of representatives for $G/K^*$ which is linearly independent over $K$ $\Leftrightarrow$ any set of representatives for $G/K^*$ is a vector space basis of $F$ over $K$.*

For any subset $S$ of a field $F$ and $n \geq 1$, let $\mu_n(S) = \{x \in S \mid x^n = 1\}$. Then $\mu_n(\Omega)$ is a cyclic subgroup of $\Omega^*$; let $\zeta_n$ denote a generator of $\mu_n(\Omega)$ (a primitive $n$-th root of unity in $\Omega$). The separable $G$-Kneser extensions are characterized as follows:

**1.14 Theorem** (Kneser's criterion) [[1], Theorem 2.6]. *Let $K \subseteq F$ be a finite separable $G$-radical extension with $G/K^*$ finite. Then $K \subseteq F$ is $G$-Kneser if and only if for any odd prime $p$, $\mu_p(G) = \mu_p(K)$ and $1 + \zeta_4 \in G$ implies $\zeta_4 \in K$.*

In what follows, we fix an extension $F/K$ and $K^* \leq G \leq F^*$ and note:

$$\mathcal{G} = \{H \mid K^* \leq H \leq G\}.$$

The behavior of $G$-Kneser extensions with respect to subextensions and subgroups is described by [[1], 3.1 and 3.2], summarized in the following:

**1.15 Proposition.** *Let $K \subseteq F$ be a separable $G$-Kneser extension.*

a) *For any $H \subseteq \mathcal{G}$, the extension $K \subseteq K(H)$ is $H$-Kneser and $K(H) \cap G = H$.*

b) *For any $E \in \mathcal{I}(F/K)$, the following are equivalent:*

(1) *$K \subseteq E$ is $H$-Kneser for some $H \in \mathcal{G}$.*

(2) *$K \subseteq E$ is $E^* \cap G$-Kneser*

(3) *$E \subseteq F$ is $E^*G$-Kneser.*

A finite $G$-radical extension is said to be strongly $G$-Kneser if, for any $E \in \mathcal{I}(F/K)$, $E \subseteq F$ is $E^*G$-Kneser. If $F/K$ is an extension and $K^* \leq G \leq F^*$, define the following natural and inclusion preserving maps:

$$\alpha : \mathcal{I}(F/K) \to \mathcal{G},\ \alpha(E) = E \cap G,\ \forall E \in \mathcal{I}(F/K)$$
$$\beta : \mathcal{G} \to \mathcal{I}(F/K),\ \beta(H) = K(H),\ \forall H \in \mathcal{G}.$$

A characterization of $G$-Kneser extensions for which these maps are inverse to each other is given by [[1], Th. 3.7], in terms of $n$-purity: If $n \in \mathbb{N}^*$, the extension $F/K$ is called $n$-pure if for any $p$ dividing $n$, $p$ odd prime or $p = 4$, one has $\mu_p \subseteq K$.

**1.16 Theorem.** *The following assertions are equivalent for a finite separable $G$-radical extension $K \subseteq F$ with $G/K^*$ finite:*

(1) *$K \subseteq F$ is strongly $G$-Kneser* (*cf.* 1.15).

(2) *$K \subseteq F$ is $G$-Kneser and $\alpha$ and $\beta$ are isomorphisms of lattices, inverse to each other.*

(3) *$K \subseteq F$ is $n$-pure, where $n = \exp(G/K^*)$.*

(For a finite group $\Gamma$ with neutral element $e$, the *exponent* of $\Gamma$ is $\exp(\Gamma) = \min\{n \geq 1 \mid x^n = e,\ \forall (x \in \Gamma\})$.

**1.17 Definition.** [[1], Def. 3.8] A field extension is called $G$-Cogalois if it is a separable strongly $G$-Kneser extension.

The lattice $\mathcal{S}(G/K^*)$ of subgroups of $G/K^*$ is isomorphic to the lattice $\mathcal{G} = \{H \mid K^* \leq H \leq G\}$. From the previous theorem one obtains:

*If $F/K$ is a $G$-Cogalois extension, then $\mathcal{I}(F/K)$ and $\mathcal{S}(G/K^*)$ are lattice isomorphic.*

Let $\Gamma$ be a group. We say, following [1], that $F/K$ is an extension with $\Gamma$-Cogalois correspondence if there is a lattice isomorphism between $\mathcal{I}(F/K)$ and $\mathcal{S}(\Gamma)$. So, a $G$-Cogalois extension $F/K$ is an extension with $G/K^*$-Cogalois correspondence.

From the theorem 1.8 we deduce:

**1.18 Theorem.** *Let $F/K$ be an extension with $\Gamma$-Cogalois correspondence for some abelian group $\Gamma$ (for instance, a strongly $G$-Kneser separable extension, where $K^* \leq G \leq T(F/K)$). The following conditions are equivalent:*

a) *There exists $L \in \mathcal{I}(F/K)$, $K \neq L \neq F$, such that $L$ is reduced in $F$ over $K$.*

b) *There exists a prime number $p$ such that $\Gamma$ is a cyclic $p$-group.*

c) *$\mathcal{I}(F/K)$ is a chain.*

d) *Every proper intermediate extension is reduced in $F$ over $K$.*

**Proof.** There exists an intermediate field $L$ reduced in $F$ over $K$, $K \neq L \neq F$, if and only if $\Gamma$ has a reduced subgroup. Since $\Gamma$ is an abelian group, 1.8 shows that it must be a cyclic $p$-group. □

**1.19 Remark.** This theorem is applicable to a wide class of finite extensions $K \subseteq F$, not necessarily Galois, including the following (see [1]):

a) *Kummer extensions with few roots of unity:* there exists $A \subseteq F$ and $n \in \mathbb{N}^*$ such that $a^n \in K$, $\forall a \in A$, $K(A) = F$ and $\mu_n(F) \subseteq \{-1, 1\}$.

b) *Generalized neat presentations*: there exist $r \in \mathbb{N}^*$, $n_1, ..., n_r \in \mathbb{N}^*$, $a_1, ..., a_r \in K^*$ such that $F = K(\sqrt[n_1]{a_1}, ... \sqrt[n_r]{a_r})$, $e(K), n) = 1$ and $\mu_p(\Omega) \subseteq K$, for any $p$ dividing $n$ ($p$ odd prime or $p = 4$), where $n$ is the least common multiple of $n_1, ..., n_r$. Here $e(K)$ is the characteristic exponent of $K$: $e(K) = \mathrm{char}(K)$ if $\mathrm{char}(K) > 0$; $e(K) = 1$ if $\mathrm{char}(K) = 0$.

Next, we investigate some properties of *inseparable extensions* having reduced subextensions. If $F/K$ is an algebraic extension, let $S$ denote the separable closure of $K$ in $F$ and $I$ the purely inseparable closure of $F$ in $K$. It is known that: *$S$ and $I$ are linearly disjoint, $S \cap I = K$ and $F/S$ is purely inseparable.* The extension $F/K$ is said to *split* if $SI = F$. Also, *$F/K$ splits if and only if $F/I$ is separable* [[7], Th. 14.16]. *If $F/K$ is normal, then $F/K$ splits: $SI = F$* [[5], Th. 4.23].

**1.20 Proposition.** *Let $F/K$ be algebraic and split ($F = SI$). If there exists $L \neq K$ reduced in $F$ over $K$, then either $F/K$ is separable or $F/K$ is purely inseparable.*

**Proof.** There are the following four possibilities:

i) $L \subseteq S$ and $L \subseteq I$. Then $L \subseteq S \cap I = K$, so $L = K$ and this is excluded.

ii) $L \subseteq S$ and $I \subseteq L$. Then $I \subseteq S$ and so $I = K$. Since $F/K$ splits, $F$ is separable over $I = K$.

iii) $S \subseteq L$ and $L \subseteq I$. Then $S \subseteq I$, so $S = K$, which means $F/K$ is purely inseparable.

iv) $S \subseteq L$ and $I \subseteq S$. Then $SI \subseteq L$, so $L = K$, contradiction. □

**1.21 Corollary.** *If $F/K$ is a normal algebraic extension and there exists an intermediate field $L \neq K$ reduced in $F$ over $K$, then $F/K$ is either separable or purely inseparable.* □

So, if $F/K$ is finite, normal and has a proper reduced intermediate field, then $F/K$ is finite and Galois (and Th. 1.11 applies) or is purely inseparable.

## 2 Primitive extensions

In [2] the following definition is given:

**2.1. Definition.** [[2], Definition 2.1] Let $L \in \mathcal{I}(F/K)$. Then $L$ is said to be:

- semi-primitive in $F$ over $K$ if $\forall c, d \in L$, $\mathrm{Irr}(c, K) = \mathrm{Irr}(d, K)$ implies $K(c) = K(d)$.
- primitive in $F$ over $K$ if $L$ is semi-primitive in $F$ over $K$ and $\forall c, d \in F \backslash L$, $\mathrm{Irr}(c, K) = \mathrm{Irr}(d, K)$ implies $K(c) = K(d)$.

We remark that the condition "$L$ is semi-primitive in $F$ over $K$" depends only on $L$ (and not on $F$) and is equivalent to "$L$ is primitive in $L$ over $K$". If this is the case, we say shortly "$L/K$ is primitive". We call $c$ and $d$ conjugate over $K$ if $c$ and $d$ have the same minimal polynomial over $K$.

**2.2. Example.** a) Every purely inseparable extension $F/K$ is primitive, because every $c \in F$ is its only conjugate over $K$.

b) Every algebraic extension of a finite field is primitive: if $c$ is algebraic over the finite field $K$, then $K(c)$ is the splitting field of $\mathrm{Irr}(c, K)$ and hence is equal to $K(d)$, for every conjugate $d$ of $c$ over $K$.

c) Every extension $F/K$ that has $\mathcal{I}(F/K)$ a chain is primitive: if $c, d \in F$ have the same minimal polynomial $g$ over $K$, then $[K(c) : K] = [K(d) : K] = \deg g$ and this implies $K(c) = K(d)$ since there is at most one extension of a given degree over $K$ in the chain $I(F/K)$. In particular, the extensions of prime degree are primitive.

**2.3. Proposition.** *Let $F/K$ be an extension of fields. Then:*

a) *$F/K$ is primitive $\Leftrightarrow$ $E \in (F/K)$, $E/K$ is primitive $\Leftrightarrow$ $\forall E \in \mathcal{I}(F/K)$, $E$ is primitive in $F$ over $K$.*

b) *If $F/K$ is primitive and $E \in \mathcal{I}(F/K)$, then $F/E$ is primitive.*

**Proof.** a) Suppose $F/K$ is primitive and let $E \in \mathcal{I}(F/K)$, $c, d$ elements in $E$ (or in $F \setminus E$). If $c$ and $d$ are conjugate over $K$, then $K(c) = K(d)$, so $E$ is primitive in $F$ over $K$. The converse is evident.

b) Let $c, d \in F$ with the same minimal polynomial $g$ over $E$. We have to show that $E(c) = E(d)$. Let $\gamma = \mathrm{Irr}(c, K) \in K[X]$ and $\delta = \mathrm{Irr}(d, K) \in K[X]$. Obviously, $g$ divides $\gamma$ and $\delta$ (in $E[X]$), so $\gcd(\gamma, \delta)$ is not a unit in $E[X]$. But the gcd of $\gamma$ and $\delta$ is obtained by Euclid's algorithm and is the same in $E[X]$ and $K[X]$, so the irreducible monic polynomials $\gamma$ and $\delta$ are equal since they have a nontrivial common factor. Since $F/K$ is primitive, we have $K(c) = K(d)$. So $E(c) = E(K(c)) = E(K(d)) = E(d)$. $\square$

**2.4. Remark.** If in the chained extensions $K \subseteq E \subseteq F$, $E/K$ is primitive and $F/E$ is primitive, then $F/K$ is not necessarily primitive. Take for instance $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega$ is a primitive third root of unity: $\mathrm{Irr}(\omega, \mathbb{Q}) = X^2 + X + 1$. Then $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ are conjugate over $\mathbb{Q}$, but generate different extensions, so $F/K$ is not primitive. But $E/K$ and $F/E$ are primitive, having prime degrees. This example also shows that a finite extension having a square free degree is not automatically primitive, as claimed in [[2], Proposition 2.3].

## References


[1] Albu, T., Nicolae, F.: *Kneser Field Extensions with Cogalois Correspondence,* J. Number Theory 52 (1995), 299-318.

[2] Alkhamees, Y., Mordeson, J.: *Reduced fields, primitive and fuzzy Galois theory,* J. Fuzzy Math., vol. 8, No. 1 (2000), 157-173.

[3] Hall, M., Jr.: *The Theory of Groups*, Macmillan, New York, 1959.

[4] Huppert, B.: *Endliche Gruppen* I, Springer Verlag, Berlin 1967.

[5] Morandi, P. : *Field and Galois Theory,* Springer Verlag 1996.

[6] Mordeson, J.N.: *Fuzzy Galois theory,* J. Fuzzy Math.(1993), 659-671.

[7] Spindler, K.: *Abstract Algebra with Applications,* vol. II, Marcel Dekker, 1990.

[8] Šafarevič, I.R.: *Construction of fields of algebraic numbers with given solvable groups,* Izv. Akad. Nauk SSSR 18 (1954), 525-578 (Russian), English translation in Amer. Math. Soc. Transl. 4 (1956), 185-237.

[9] Volf, A.C., Tofan, I.: *Fuzzy Intermediate Fields and Reduced Extensions,* in Advances in Generalized Structures, Approximate Reasoning and Applications, Performantica Press 2001, 91-96.

Faculty of Mathematics,
"A.-I. Cuza" University ,
6600 Iasi,
Romania
e-mail: volf@uaic.ro