Can. J. Math., Vol. XXXIX, No. 5, 1987, pp. 1025-1037

# ON THE GALOIS THEORY OF COMMUTATIVE RINGS II: AUTOMORPHISMS INDUCED IN RESIDUE RINGS

CARL FAITH

**1. Introduction.** Let $G$ be a group of automorphisms of a commutative ring $K$, and let $K^G$ denote the Galois subring consisting of all elements left fixed by every $g$ in $G$. An ideal $M$ is *G-stable*, or *G-invariant*, provided that $g(x)$ lies in $M$ for every $x$ in $M$, that is, $g(M) \subseteq M$, for every $g$ in $G$. Then, every $g$ in $G$ induces an automorphism $\bar{g}$ in the residue ring $\bar{K} = K/M$, and if $\bar{G}$ is the group consisting of all $\bar{g}$, trivially

$$(1) \qquad \bar{K}^{\bar{G}} \supseteq \overline{K^G}.$$

When the inclusion (1) is strict, then $G$ is said to be *cleft at* $M$, or by $M$, and otherwise $G$ is *uncleft at* (by) $M$. When $G$ is cleft at all ideals except 0, then $G$ is *cleft*, and *uncleft* otherwise.

The main results on uncleft groups are for $G$ locally finite in the sense that orbit number $n(x) = |Gx| < \infty$ for every $x$ in $K$. Below let $L(G, M)$ be the inverse image of $\bar{K}^{\bar{G}}$ under the canonical map $K \to \bar{K} = K/M$.

1. THEOREM. *If $G$ is a locally finite automorphism group of $K$, and if $M$ is a $G$-invariant ideal, then $\bar{K}^{\bar{G}}$ is radical-torsion over $K^G$; that is, if $x \in \bar{K}^{\bar{G}}$, and if $n = |Gx|$, then*

$$\bar{x}^n \in \overline{K^G} \quad \text{and} \quad n\bar{x} \in \overline{K^G}.$$

2. COROLLARY. *If $G$ is a locally finite automorphism group of $K$ with unit orbit lengths, or if $K$ is generated by*

$$\{x^{|Gx|} | x \in K\},$$

*then $G$ is uncleft. Moreover, if $M$ is a maximal ideal such that $\bar{K} = K/M$ has characteristic not dividing $|Gx| \forall x \in L(G, M)$, then $G$ is uncleft at $M$.*

Employing Kaplansky's theorem on the structure of radical extensions of fields in the same way as in [5], we obtain:

Received April 13, 1984. This paper is dedicated to Sam Perlis, teacher and friend.

3. THEOREM. *If $G$ is locally finite and cleft at a maximal ideal $M$, then the residue field $\bar{K} = K/M$ has prime characteristic $p$, and $p$ divides $|Gx|$ for all $x$ in $L(G, M)$ not in $K^G + M$. Moreover,*

$$x^{p^{e(x)}} \in K^G + M,$$

*where $e(x)$ is the exponent of $p$ in $|Gx|$.*

A subfield $B$ of a field $A$ is *relatively perfect* if $A$ contains no purely inseparable extension of $B$ (other than $B$).

4. COROLLARY. *Let $G$ be locally finite on $K$, and $M$ a $G$-invariant maximal ideal. Then*:

(1) *If $\bar{K}^G$ is a relatively perfect subfield of $\bar{K} = K/M$, then $G$ is uncleft at $M$.*

(2) *If $G$ has unit orbit lengths (resp. if $|Gx| \notin M$ for all $x \in K$), then $G$ is uncleft (resp. uncleft at $M$).*

A number of these results are implicit in [**5**], but under various restrictions such as $G = (g)$ cyclic, $M$ a point annihilator ideal, and the requirement throughout that $G$ is a linearly independent group of automorphisms, all of which obscure the generality and beauty of the theorems. We therefore give complete proofs here, and also investigate local properties of uncleftness, e.g.: Example 6, which shows that uncleftness at prime ideals does not imply uncleftness; and Theorem 7, which shows that uncleftness at a $G$-stable ideal $P$ implies uncleftness of the extended group at the maximal ideal of the local ring at $P$. As an application, we prove that any Galois group $G$ ( [**1**], [**2**] ) is cleft.

Our results also yield other specific information on the nature of Galois groups. It is known that a finite group $G$ of automorphisms of $K$ is a Galois group provided that for every $1 \neq g \in G$ and every maximal ideal $M$ of $K$ there is an element $x \in K$ so that $g(x) - x \in M$ ( [**2**] ). Thus, if $G$ is not a Galois group, and if

$$g(x) - x \in M \quad \text{for all } x \in K \quad [\bar{g}(M) = 1]$$

then either (1)

(1) $\qquad K = K^g + M$

or else

(2) (2a) $\bar{K} = K/M$ has prime characteristic $p|n$ and

(2b) $\bar{K}$ is purely inseparable over $\bar{K}^g$ of exponent equal to that of $p$ in $n$.

This shows that non-Galois groups for commutative rings bear a close resemblance to those for fields in that, excepting for the case (1) where $g$ acts trivially modulo $M$, inseparability of field extensions is necessitated. (This also shows that a non-Galois group $G$ must have $(g)$-stable maximal ideal $M$ for some $1 \neq g \in G$.)

**2. Proofs of the theorems.** If $M$ is a $G$-invariant ideal of $K$, we let

$$\pi(M):K \to \bar{K} = K/M \tag{2.1}$$

be the canonical map. Then:

$$L = L(G, M) = \pi(M)^{-1}(\bar{K}^{\bar{G}}) = \{k \in K | g(k) - k \in M \ \forall\ g \in G\}. \tag{2.2}$$

Let

$$F = \pi^{-1}(\overline{K^G}).$$

Thus,

$$L/M = \bar{K}^{\bar{G}} \text{ and } F/M = \overline{K^G}. \tag{2.3}$$

Next: $G$ induces a group $G(L)$ of automorphisms of $L$. For, if $x \in L$, and $h \in G$, then $gh(x) - x \in M$ and $h(x) - x \in M$ for all $g \in G$, and hence

$$g(h(x)) - h(x) \in M, \quad \text{for all } g \in G,$$

so $h(x) \in L$ for all $h \in G$. It follows that $L^{G(L)} = K^G$. This will be used frequently.

*Proof of Theorem* 1. Let

$$Gx = \{g_1(x), \ldots, g_n(x)\}$$

for $x \in K$ (so $n = |Gx|$). Evidently,

$$\beta = \prod_{i=1}^{n} g_i(x) \in K^G$$

and

$$\alpha = \sum_{i=1}^{n} g_i(x) \in K^G$$

the (reduced) $G$-norm $N_{Gx}(x)$ and $G$-trace $T_{Gx}(x)$ respectively of $x$. If $x \in L$, then write

$$g_i(x) = x + m_i \quad (m_i \in M)$$

for $i = 1, \ldots n$. Then, for some $m \in M$,

$$\beta = x^n + m,$$

so $x^n \in K^G + M$ as stated, and dually $nx \in K^G + M$.

*Proof of Corollary* 2. If $|Gx|^{-1} \in K$, for every $x \in L(G, M)$, then by Theorem 1 we have $L(G, M) = K^G + M$ for every ideal $M$.

Next, if $K$ is generated by $\{x^{n(x)} | x \in K\}$, then $K^G$ is generated by

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

$\{a^{n(a)} | a \in K^G\}$ (regardless of the choice of $\{n(x)\}_{x \in K}$ or $G$). Then, $\bar{K}$ is generated by $\{\bar{x}^{n(x)}\}_{x \in K}$, and $\overline{K^G}$ by $\{\bar{a}^{n(a)} | a \in K^G\}$, so Corollary 2 follows from Theorem 1.

*Proof of Theorem* 3. This is proved in the same way as the corresponding result of [5]. Using Theorem 1, we have that $\bar{K}^{\bar{G}}$ is radical (torsion) over $\overline{K^G}$. This implies that $\overline{K^G}$ is a field (along with $\bar{K}^{\bar{G}}$), for if $0 \neq a \in \overline{K^G}$, then $\bar{a}^{-1} \in \bar{K}^{\bar{G}}$. Since

$$b = (a^{-1})^n \in \overline{K^G}$$

for some $n$, then

$$\bar{a}^{-1} = \bar{a}^{n-1}\bar{b} \in \overline{K^G}.$$

We may now apply Kaplansky's characterization [7] of radical field extensions $F/H$ when $F \neq H$. Then: $F$ has characteristic $p > 0$ and either

(KAP 1) $F$ is an algebraic extension of $P = GF(p)$

or

(KAP 2) $F$ is purely inseparable over $H$.

The converse also holds: (Kap 2) is a radical extension by definition. Furthermore, if $x$ is in $F$ in (Kap 1), then $P(x)$ is a finite field, say $P = GF(p^m)$, so $x^{p^m} = x$. Then, $x \neq 0$ satisfies

$$x^{p^m - 1} = 1 \in P \subseteq H.$$

Moreover, in this case note that $p$ is prime to the exponent $p^m - 1$. Similarly, $p$ is prime to the smallest exponent $t > 0$ for which $x^t \in H$ when $x \notin F$. (For obviously, $t \leqq p^m - 1$, hence we may write

$$p^m - 1 = tg + r, \quad \text{for } 0 \leqq r < t,$$

and then $x^r \in F$, so $r = 0$, that is, $t$ divides $p^m - 1$, so $(p, t) = 1$.)

Thus, inasmuch as for $n = |Gx|$ we have $n\bar{x}$ and $\bar{x}^n$ both in $\overline{K^G}$, for any $\bar{x}$ in $\bar{K}^{\bar{G}}$, then when $G$ is $M$-cleft, then $\bar{x} \notin \overline{K^G}$ only if $\bar{K}$ has prime characteristic dividing $|Gx|$. This rules out (Kap 1) as a possibility, hence (Kap 2) holds as asserted. Moreover, since $(x^{p^e})^{n_0}$ lies in $K^G + M$, for any $x \in L(G, M)$, where $e$ is the exponent of $p$ in $n = |Gx|$, and $n_0 = np^{-e}$, then $x^{p^e}$ must lie in $K^G + M$, since $p$ is prime to $n_0$. This completes the proof of Theorem 3.

**3. $G$-stable ideals.** If $I$ is an ideal of $K$, then the radical $\sqrt{I}$ is a semiprime ideal; that is, an intersection of prime ideals. Moreover, $\sqrt{I}$ is $G$-stable if $I$ is.

We say that $K$ is *$G$-simple* provided that $K$ has no $G$-stable ideals except the trivial ones.

5. PROPOSITION. *Let $M$ be a $G$-stable ideal of $K$. Then*:

(1) $\sqrt{M}$ *is a $G$-stable semiprime ideal containing $M$.*

(2) *There exists a maximal $G$-stable ideal $P$ containing $M$.*

(3) *If $K$ is $G$-simple, then $K^G$ is a field.*

(4) *If a maximal ideal $P$ of $K$ has finite orbit under $G$, and if $K$ is $G$-simple, then $K$ is a finite product of fields; in fact,*

$$K \approx \prod_{i=1}^{n} K/g_i(P),$$

*where the orbit of $P$ under $G$ is $\{g_i(P)\}_{i=1}^n$, and $K^G$ embeds in each direct factor of $K$.*

(5) *If $P$ is a maximal $G$-stable ideal containing $M$, then $\bar{K} = K/P$ is $\bar{G}$-simple for the induced group $\bar{G}$. Moreover,*

$$\bar{K}^{\bar{G}} = L(G, P)/P$$

*is a field, hence $P \cap L(G, M)$ is a prime ideal of $L(G, M)$.*

*Proof.* With the possible exception of (4), these are trivial consequences of the definition, e.g., (1) follows from the remark preceding the proposition, (2) by Zorn's Lemma, (3) by virtue of the fact that a $G$-stable ideal $P$ is a maximal $G$-stable ideal if and only if $\bar{K} = K/P$ is $\bar{G}$-simple. In this case, $\bar{K}^{\bar{G}}$ is a field, since for any $0 \neq a \in \bar{K}^{\bar{G}}$, the ideal $a\bar{K}$ is $\bar{G}$-stable, whence equals $\bar{K}$. Thus, $a$ is a unit of $\bar{K}$, and then $a^{-1} \in \bar{K}^{\bar{G}}$, so $\bar{K}^{\bar{G}}$ is a field. Inasmuch as

$$\bar{K}^{\bar{G}} = L(G, P)/P$$

in virtue of the definition of $L(G, P)$, then $L(G, P)/P$ is a field. Since

$$L(G, M) \subseteq L(G, P),$$

then $L(G, M)/(L(G, M) \cap P)$ is an integral domain, so (5) holds.

(4) follows in the same way as in [**8**] for a cyclic group $G$: since

$$\bigcap_{i=1}^{n} g_i(P)$$

is $G$-stable, it is $= 0$, hence $K$ embeds in the product of the $K/g_i(P)$, and the embedding is an isomorphism by the Chinese Remainder Theorem.

6. *Example.* We present a cleft group $G$ uncleft at every prime ideal.

An example given in [**2**] suffices. Let $K = F + Fx + Fy$ be the vector space of dimension 3 over a field $F$ and make $K$ into a local ring with unique prime ideal $P = Fx + Fy$ be decreeing that

$$xy = yx = x^2 = y^2 = 0.$$

Consider the automorphism group $G = (g)$, where $g(x) = y$ and $g(y) = x$. Then $K^G = F + M$, where

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

$$M = (x + y)K = (x + y)F.$$

Suppose now that F has characteristic 2. Then, $L(G, M) = K$ since

$$g(x) - x = y - x = y + x \in M$$

and

$$g(y) - y = x - y = x + y \in M.$$

Thus,

$$K = L(G, M) \neq K^G = F + M$$

so $G$ is cleft at $M$, but uncleft at $P$ since

$$K = F + P = K^G + P.$$

**4. Localization at prime ideals.** A subtlety of Theorem 7 is that the $G$-stable ideal $P$ is required to be prime in (1) but merely to contract to a prime ideal of $K^G$ in (2).

7. THEOREM. *Let $G$ be a locally finite group of automorphisms of $K$.*

(1) *The local ring of $K$ at a $G$-stable prime ideal $P$ is canonically the localization of $K$ at the contracted ideal $P_0$ of $P$ to $A = K^G$. Thus, if $T = K\backslash P$, and $S = A\backslash P_0 = T \cap A$, then:*

$$(7.1) \quad K_P = KT^{-1} = KS^{-1} = K_{P_0}.$$

(2) *Here and below, let $P$ be any $G$-stable ideal of $K$ that contracts to a prime ideal $P_0$ of $A = K^G$, and let $G^{\mathrm{ex}}$ denote the canonical extension of $G$ to*

$$Q = KS^{-1} = K_{P_0}.$$

*Then, the Galois subring of $G^{\mathrm{ex}}$ is*

$$(7.2) \quad Q^{G^{\mathrm{ex}}} = A_{P_0} = AS^{-1}.$$

(3) *Furthermore, $PQ = PS^{-1}$, and if $L = L(G, P)$, then*

$$(7.3) \quad L(G^{\mathrm{ex}}, PS^{-1}) = LS^{-1}$$

*hence*

$$(7.4) \quad \bar{Q}^{\overline{G^{\mathrm{ex}}}} = \overline{LS}^{-1}$$

*where $\bar{Q} = Q/PQ$.*

(4) *Finally, if $G$ is uncleft at $P$, then $G^{\mathrm{ex}}$ is uncleft at $PQ$, so that*

$$(7.5) \quad \bar{Q}^{\bar{G}} = \overline{Q^G} = \overline{LS}^{-1} = \overline{AS^{-1}}.$$

*Proof.* (1) Let $Q = K_P$, and if $g \in G$, let $g$ also denote the automorphism of $Q$ that sends $x/t$ onto $g(x)/g(t)$, for any $t \in T$, and let $G$ also denote the group $G^{\mathrm{ex}}$ of such extensions. Then the extended group $G$ is also

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

locally finite, and for any $x \in Q$, if $n = |G|$, then there are $n$ "symmetric functions" $\sigma_1, \ldots, \sigma_n$ such that

$$\sum_{g(x) \in Gx} (x - g(x)) = x^n - \sigma_1(x)x^{n-1} + \ldots + (-1)^n\sigma_n(x) = 0.$$

Now, if we let $F = Q^G$, then $a_i = \sigma_i(x) \in F$, $i = 1, \ldots, n$, with

$$a_1 = \sum_{g(x) \in Gx} g(x) = T_G(x), \quad \text{and} \quad a_n = \prod_{g(x) \in Gx} g(x) = N_G(x)$$

the $G$-trace and $G$-norm respectively of $x$. Trivially, $x$ is a unit of $Q$ if and only if $a_n$ is a unit. In this case,

$$x^{-1} = a_n^{-1}(x^{n-1} - a_1x^{n-2} + \ldots + (-1)^{n-1}a_{n-1}). \tag{7.6}$$

In particular, for $x = t/1 \in Q$, this shows that $1/t \in KS^{-1}$, that is, that (7.1) holds.

(2) Let $k/s \in Q$, for $s \in S$, and $k \in K$. Then $k/s \in Q^{G^{\text{ex}}}$ if and only if

$$(g(k) - k)/s = 0 \quad \text{for all } g(k) \in Gk.$$

Since $|Gk| < \infty$, this happens if and only if there exists $t \in S$ such that

$$(g(k) - k)t = 0 \quad \text{for all } g(k) \in Gk.$$

But then $g(kt) = kt$, for all $g$ in $G$, so this implies that $kt$ lies in $A = K^G$. Then $k/1$, whence $k/s$, belongs to $AS^{-1}$, proving (7.2).

(3) Let $k/s$ be an element of $L(G^{\text{ex}}, PS^{-1})$. Since $g(k/s) = k/s$, then

$$g(k)/s - k/s \in PS^{-1} \quad \text{for all } g \in G$$

hence,

$$g(k)/1 - k/1 \in PS^{-1} \quad \text{for all } g \in G$$

and the latter holds if and only if there is a $t$ in $S$ such that

$$(g(k) - k)t \in P \quad \text{for all } g \in G,$$

equivalently,

$$g(kt) - kt \in P$$

so that $kt \in L$, when $k/1 \in LS^{-1}$, proving that

$$L(G^{\text{ex}}, PS^{-1}) = LS^{-1}.$$

Now the reverse inclusion is trivial, hence (7.3), whence (7.4), holds.

(4) If $G$ is uncleft at $P$, then $L = A + P$, so by (7.3)

$$L(G^{\text{ex}}, PS^{-1}) = LS^{-1} = AS^{-1} + PS^{-1}$$

hence, by (7.4)

$$\bar{Q}^{\bar{G}} = \overline{AS}^{-1}.$$

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

Since obviously

$$\bar{Q}^{\bar{G}} \supseteq \overline{Q^G} \supseteq \overline{AS^{-1}}$$

we get (7.5).

8. THEOREM. *If the extended group $G^{\mathrm{ex}}$ of a group $G$ of $K$ is cleft at the maximal ideal $M$ of the local ring $K_P$ of a $G$-stable prime ideal $P$, then $\bar{K} = K/P$ has prime characteristic $p$ and*

$$\bar{k}^{p^e} \in \overline{K^G} \quad \forall \bar{k} \in \bar{K}^{\bar{G}}$$

*where $e$ is the exponent of $p$ in $|Gk|$. (If $|Gx|$ is prime to $p$, then $\bar{k} \in \overline{K^G}$.)*

*Proof.* By Theorem 3,

$$\bar{q}^{p^e} \in \overline{Q^G} \quad \text{for all } \bar{q} \in \bar{Q}^{\bar{G}},$$

where $e = e(q)$ is the exponent of $p$ in $|Gq|$, and $\bar{Q} = Q/PS^{-1}$, etc. In particular, for $k \in K$, we have

$$\overline{k/1}^{p^e} = \bar{k}^{p^e}/1 \in \overline{Q^G} = \overline{K^G(S^G)^{-1}}$$

so it follows that

$$\bar{k}^{p^e} \in \overline{K^G},$$

for the exponent $e$ of $p$ in $|Gk|$. (If $p$ is prime to $|Gk|$, then $\bar{k} \in \overline{K^G}$ by Corollary 2 or Theorem 3.)

**5. Two classical lemmas.** The first conclusion in the next lemma is classical, and the second follows from Proposition 5.

9. LEMMA. *If $K$ is finitely generated projective over $A = K^G$, then any prime ideal $P_0$ of $A$ is the contraction of a maximal $G$-stable ideal $P$ of $K$. Moreover, if $M$ is a $G$-stable ideal of $K$ contained in $P$, and if $L = L(G, M)$, then $P_1 = P \cap L$ is a prime ideal of $L$, and hence $P_0$ is the contraction of a prime $G(L)$-invariant ideal of $L$, where $G(L)$ is the group induced by $G$ in $L$.*

*Proof.* Since $P_0K$ is $G$-stable, then $P$ exists by Proposition 5 provided only that $P_0K \neq K$. The hypothesis on $K/A$ implies that $K$ generates mod-$A$, and this, together with flatness of $K$ over $A$, implies that $P_0K \neq K$. For flatness allows us to identify $P_0K$ with $P_0 \otimes_A K$. Now $K^n \to A \to 0$ is exact for some $n$, hence the canonical sequence

$$P_0 \otimes_A K^n \approx (P_0 \otimes_A K)^n \to P_0 \otimes_A A \to 0$$

is exact, so

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

$$P_0 \otimes_A K \approx P_0 K = K$$

implies

$$P_0 \otimes_A A \approx P_0 = A,$$

contrary to the choice of $P_0$.

The next lemma is a corollary to a theorem of Vasconcelos [**11**] on epimorphic endomorphisms of finitely generated modules (they are automorphisms).

10. Lemma. *Let $K$ be a commutative ring with subrings $L \supseteq A$ such that for some ideal $M$, $\bar{K} = K/M$ is a free module of finite rank $n$ over $\bar{L}$. Then, if $K$ is generated as an $A$-module by $n$ elements, then $L + M = A + M$.*

*Proof.* Let $\bar{L}$ and $\bar{A}$ be the images of $L$ and $A$ resp. under $K \to \bar{K}$. If $\{\bar{u}_i\}_{i=1}^n$ is a free basis of $\bar{K}$ over $\bar{L}$ and $\{x_i\}_{i=1}^n$ generates $K$ over $A$, then $\{\bar{x}_i\}_{i=1}^n$ generates $\bar{K}$ over $\bar{A}$, hence over $\bar{L}$, and consequently there is an epimorphism $f$ of the $\bar{L}$-module $\bar{K}$ sending $\bar{u}_i$ onto $\bar{x}_i$ $\forall$ $i \leqq n$. However, Vasconcelos' Theorem [**4**] implies that $f$ is an automorphism so $\{\bar{x}_i\}_{i=1}^n$ is a free basis of $\bar{K}$ over $\bar{L}$, hence is a free basis of $\bar{K}$ over $\bar{A}$. Then trivially $\bar{L} = \bar{A}$.

**6. The maximal ideal criterion for a Galois group.** A group $G$ is said to be *faithful modulo a $G$-stable ideal $M$* provided that $G$ is canonically isomorphic to the induced group $\bar{G}$ of the residue ring $\bar{K} = K/M$. Then, $G$ acts faithfully on the residue ring $K/M$.

A theorem of [**2**] states that a finite group $G$ of automorphisms of $K$ is a Galois group in the sense of [**1**] if and only if for every maximal ideal $M$ (not necessarily $G$-stable) and every element $1 \neq g \in G$ there is an element $x$ in $K$ so that $g(x) - x \notin M$. (1)-(3) below are some evident corollaries of the Galois group criterion just stated; (4) is Lemma 1.7 of [**2**].

11. Corollaries From The Maximal Ideal Criterion. *Let $G$ be a Galois group of $K$.*

(1) *$G$ is independent.*

(2) *If $M$ is any $G$-stable ideal $\neq K$, then $G$ acts faithfully on the residue ring $\bar{K} = K/M$ and, moreover, the induced group $\bar{G}$ is a Galois group of $\bar{K}$.*

(3) *Any subgroup $H$ of $G$ is a Galois group of $K$, and if $H$ is a normal subgroup, then $G/H$ induces a Galois group of $K^H$ over $K^G$.*

(4) *If $B$ is an algebra over $A = K^G$, and $G^{\text{ex}}$ extends $G$ naturally to $K \otimes_A B$, then $G^{\text{ex}}$ is a Galois group with Galois subring $B$.*

12. Lemma. *If $G$ is a Galois group of $K$, and if $M$ is a $G$-stable ideal for which $L = L(G, M)$ is a local ring, then $G$ is uncleft at $M$.*

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

*Proof.* By (2.4), the group $G$ induces a group $G(L)$ of automorphisms in $L$, and

$$A = K^G = L^{G(L)}.$$

Since a Galois subring of a local ring is a local ring, then $A$ is local. Since $\bar{L} = L/M$ is a homomorph of $L$, it too is a local ring. By Corollary 11, $G$ induces a Galois group $\bar{G}$ in $\bar{K}$ of same order. Since $\bar{L}$ and $A$ are local rings, then $\bar{K}$ is free over $\bar{L}$ of rank $n = |G|$, and $K$ is free of same rank over $A$. Then, Lemma 10 yields the desired equality $L = A + M$.

13. COROLLARY. *A Galois group is uncleft.*

*Proof.* The proof proceeds via localization employing Proposition 5, Corollary 11, and Lemma 12. Let $L = L(G, M)$ for a $G$-stable ideal $M$, and let $A = K^G$, and $B = A + M$. Then $G$ is uncleft at $M$ if and only if $L_{P_0} = B_{P_0}$ for every maximal ideal $P_0$ of $A$; equivalently,

$$LS^{-1} = BS^{-1} \quad \text{for every } S = A \setminus P_0.$$

Now, $P_0K$ is contained in a maximal $G$-invariant ideal $P$ by Proposition 5 and $P \cap A = P_0$ by maximality of $P_0$ in $A$. Note if $M$ is not contained in $P$, then $M$ contains an element of $S$, and this implies that $MS^{-1} = KS^{-1}$, whence $LS^{-1} = BS^{-1}$. (If $1 = m + p$ for elements $m \in M$ and $p \in P$, then the $G$-norm $N(p)$ of $p$ is in $P_0$, and $N(p) - 1 = s \in S \cap M$.)

Thus, we may suppose that $P \supseteq M$, and hence by Proposition 5 that $P_1 = L \cap P$ is a prime ideal of $L$. Moreover, by Theorem 7 (1), the localization of $L$ at $P_1$ is that of $A$ at $P_0$ inasmuch as $A$ is the Galois subring of $L$ corresponding to $G(L)$ induced by $G$. This shows that the subring $LS^{-1}$ of $KS^{-1}$ is a local ring $\approx L_{P_1}$. Now trivially

$$LS^{-1} = L(G^{\text{ex}}, MS^{-1})$$

and by Lemma 12 the right side is equal to $AS^{-1} + MS^{-1}$, since, by (7.2), $AS^{-1}$ is the Galois subring of $Q = KS^{-1}$ corresponding to the extended group $G^{\text{ex}}$, and $G^{\text{ex}}$ is a Galois group by Corollary 11 (4).

14. THEOREM. *If $G$ is a finite simple group for a local ring $K$, then one of the following conditions holds*:

(1) *$G$ is a Galois group.*

(2) *$G$ is a cleft at $J = \max K$.*

(3) $K = K^G + J = K^g + J \quad \forall g \in G$.

*Proof.* Let

$$H = \{g \in G | \bar{g} = 1 \text{ in } \bar{K} = K/J\}.$$

Since $K$ is local, then $G$ is a Galois group if and only if $H = 1$. Thus, if (1) fails, by simplicity of $G$, and normality of $H$, then $\bar{G} = 1$, so $\bar{K} = \bar{K}^{\bar{G}}$. Thus, $G$ is uncleft at $J$ if and only if $\bar{K} = \overline{K^G}$, that is, if and only if $K = K^G + J$. Then $K = K^g + J$, for any $g \in G$.

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

15. COROLLARY. *Let $K$ be a local ring. If $G$ is a finite simple group either of unit order or $\bar{K}$ has characteristic not dividing $|G|$, then $G$ is a Galois group if and only if $K \neq K^g + J$ for any $1 \neq g \in G$.*

*Proof.* Since $G$ is uncleft, the theorem applies.

16. *Example.* We present an independent uncleft group not Galois. Let $F$ be a field of characteristic $\neq 2$, and let $K = F\langle x, y\rangle$ be the power series ring in two variables. Then $K$ is local and $J = (x, y)$. Let $g$ denote the switching automorphism. Then $K^g \supseteq F$, so $K = K^g + J$. Note $(g)$ is not a Galois group since $\bar{g} = 1$ in $\bar{K}$. However, $(g)$ is uncleft since $|g| = 2$ is a unit. Furthermore, $(g)$ is independent since $K$ is a domain.

17. COROLLARY. *If $G$ is any group for any commutative ring, and if both $K$ over $K^G$, and $\bar{K} = K/M$ over $\bar{K}^{\bar{G}}$ are free of equal ranks, or $\bar{K}$ over $\bar{K}^{\bar{G}}$ is free of rank $n$ and $K$ is generated over $K^G$ by $\leqq n$ elements, then $G$ is uncleft at $M$.*

*Proof.* Apply Lemma 10.

We say that a group $G$ of automorphisms of $K$ is *weakly pre-Galois* provided that $G$ is a finite group of order $n$ and $K$ is generated over $K^G$ by $n$ elements as a $K^G$-module.

18. THEOREM. *If $M$ is a maximal ideal of $K$, and if $G$ is weakly pre-Galois, then $G$ is uncleft at $M$.*

*Proof.* Since $G \approx \bar{G}$, then

$$[\bar{K}:\bar{K}^{\bar{G}}] = n = |G|$$

holds by the Galois Theory for fields. Moreover, since $K$ is generated by $n$ elements over $K^G$, then Lemma 10 applies.

19. COROLLARY. *Let $G$ be a finite group of automorphisms, and $M$ a maximal ideal of $K$ satisfying one of the following conditions:*

(A) *$n = |G|$ is a unit of $K/M$, that is, $n \notin M$.*

(B) *$\bar{K} = K/M$ is not purely inseparable over $\overline{K^g}$ for any $1 \neq g \in G$ unless $K = K^g + M$.*

(C) *$\bar{K}$ has characteristic not dividing $n$.*

(D) *$\bar{K}$ has characteristic 0.*

(E) *$\bar{K}$ is absolutely algebraic.*

*Then, for any $g \in G$, $g(x) - x \in M$ for all $x \in K$ if and only if $K = K^g + M$.*

*Proof.* This is an application of Theorem 3, and Corollary 4, inasmuch as the condition $g(x) - x \in M$ for all $x$ in $K$ implies that

$$L((g), M) = K,$$

https://doi.org/10.4153/CJM-1987-052-9 Published online by Cambridge University Press

and hence that $K \neq K^g + M$ if and only if $(g)$ is cleft at $M$. Since each of the conditions imply that $(g)$ is uncleft, the result follows.

The corollary implies the statements of the last two paragraphs of the introduction.

*Problems.* 1. What about locally infinite automorphism groups of $K$? What is the relation between $\bar{K}^{\bar{G}}$ and $\overline{K^G}$ in general? What are good sufficient conditions for uncleft $G$?

2. Find an example of a quorite extension $K$ over $A = K^G$ with $K$ local (or indecomposable) and $G$ dependent.

*Notes.* 1. This paper is dedicated to Professor Sam Perlis of Purdue University, who infected me with his love of mathematics and, above all, the beauty of Galois Theory (circa 1951-5).

2. The "algebraic extension of" part was inadvertently left off of (KAP 1) in [**5**]. This in no way affects the results inasmuch as the only place it was used was to discount the possibility that $F$ is $p^e$-radical over a subfield $\neq F$.

3. All that is required in Lemma 10 and Corollary 17 is that $L$ have the property that for every $n$, every epi of $L^n \to L^n$ be an automorphism; equivalently, the matrix ring $L_n$ be *Dedekind finite* in the sense that $\phi\eta = 1 \Leftrightarrow \eta\phi = 1$. Thus matrix rings over commutative rings are Dedekind finite. Noetherian rings, and semilocal rings, are also Dedekind finite, and, hence, so are the matrix rings over them. (See, e.g., [**6**], esp. Chapter 18.) Thus, Lemma 10 and Corollary 17 also hold whenever $\bar{K}$ or $\bar{L} = \bar{K}^{\bar{G}}$ is Noetherian or semilocal, in particular, when $K$ is Noetherian or semilocal. (For then $\bar{K}$ Noetherian (semilocal), hence so is the matrix ring $\bar{K}_n$ for any $n$. Now use the fact that any subring (e.g., $\bar{L}_n$) of a Dedekind finite ring $\bar{K}_n$ is Dedekind finite.)

4. (7.1) of Theorem 7 may be expressed as saying that localization of $K$ at the prime ideal $P$ is the same as localization at a prime ideal $P_0 = K^G \cap P$ of $K^G$. For a Galois group this is contained in [**2**].

It has been pointed out that (d) of Theorem 1.3 of [**2**] gives a much shorter proof of Corollary 13.

## References


1. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. *97* (1960), 367-409.
2. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs A.M.S. *52* (1965), 15-33.
3. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Math. *181* (Springer-Verlag, Berlin, Heidelberg and New York, 1971).
4. C. Faith, *Galois extensions of commutative rings*, Math. J. Okayama U. *18* (1976), 113-116.

5. ——— *On the Galois theory of commutative rings I: Dedekind's theorem on the independence of automorphisms revisited*, in *Algebraist's Hommage*, Proceedings of the Yale Symposium in honor of Nathan Jacobson, New Haven (1981), Contemporary Math. *13* (1982), 183-192.
6. ——— *Algebra II: Ring theory* (Springer-Verlag, 1976).
7. I. Kaplansky, *A theorem on division rings*, Can. J. Math. *3* (1951), 290-292.
8. A. Shamsuddin, *Rings with automorphisms leaving no nontrivial proper ideals invariant*, Proceedings of the Conference on Algebra and Geometry, Kuwait University, Khaldiya, Kuwait.
9. W. Vasconcelos, *On local and stable cancellation*, An. Acad. Brasil, Ci *37* (1965), 389-393.
10. ——— *On finitely generated flat modules*, Trans. A.M.S. *138* (1969), 505-512.
11. ——— *Injective endomorphisms of finitely generated modules*, Proc. A.M.S. *25* (1970), 900-901.

*Rutgers University,*
*New Brunswick, New Jersey*