On cohomology of groups in finite local rings

Takao Sumiyama

* Aichi Institute Of Technology

Copyright ©1987 by the authors. Mathematical Journal of Okayama University is produced by The Berkeley Electronic Press (bepress). http://escholarship.lib.okayama-u.ac.jp/mjou
ON COHOMOLOGY OF GROUPS IN FINITE LOCAL RINGS

Dedicated to Professor Hisao Tominaga on his 60th birthday

TAKAO SUMIYAMA

Let $G$ and $H$ be finite groups and let $\rho: H \to \text{Aut}(G)$ be a fixed group homomorphism from $H$ to the automorphism group of $G$. A map $f: H \to G$ is called a crossed homomorphism if $f(ab) = \rho_a(f(b))f(a)$ for any $a, b \in H$. This is an extended definition of usual crossed homomorphism (cf. [3, pp. 104–106]). The set of all crossed homomorphisms of $H$ to $G$ will be denoted by $Z^1_\rho(H, G)$. For each fixed $x \in G$, the map $f_x: H \to G$ defined by $f_x(a) = \rho_a(x)x^{-1}$ is a crossed homomorphism. The function of this form $f_x$ is called principal, and the set of all principal crossed homomorphisms of $H$ to $G$ is denoted by $B^1_\rho(H, G)$. In case $G$ is Abelian, $Z^1_\rho(H, G)$ and $B^1_\rho(H, G)$ are Abelian groups and $H^1_\rho(H, G) = Z^1_\rho(H, G)/B^1_\rho(H, G)$ is the first cohomology group of $H$ over $G$.

When $S$ is a finite set, $|S|$ denotes the number of elements of $S$.

The purpose of this paper is to show that [7, Theorem 1 (3)] can be derived from a more general proposition and to describe finite local rings in terms of cohomology of their unit groups.

**Theorem 1.** Let $G$ be a finite solvable group with order $g$, $H = \langle c \rangle$ a cyclic group with order $h$, and $\rho: H \to \text{Aut}(G)$ a group homomorphism. If $(g, h) = 1$, then $Z^1_\rho(H, G) = B^1_\rho(H, G)$, that is, all crossed homomorphisms of $H$ to $G$ are principal.

**Proof.** Let $\widetilde{G}$ be the semidirect product of $H$ with $G$ determined by $\rho$. That is, any element $x$ of $\widetilde{G}$ is uniquely written as $x = at$ with $a \in H$ and $t \in G$, and the multiplication is given by

$$(at)(bv) = (ab)(\rho_\rho(t)v) \quad (a, b \in H, t, v \in G).$$

Note that $\rho_\rho(t) = b^{-1}tb$ in $\widetilde{G}$.

Let $f: H \to G$ be a crossed homomorphism. Then

$$(c^{f(c)})^s = c^{s\rho_{c\rho^{-1}}(f(c))\rho_{c\rho^{-1}}(f(c))...\rho_\rho(c(f(c)))f(c)} = c^{sf(c^s)}$$

for any integer $s \geq 1$, so the order of $c$ is equal to the order of $cf(c)$. As
\langle c \rangle \text{ and } \langle cf(c) \rangle \text{ are both Hall subgroups of } \overline{G}, \text{ by [1, p. 141 Theorem 9.3.1. 2]}, \text{ there exists } y = bv \in \overline{G}(b \in H, \nu \in G) \text{ such that } y^{-1}cy = (cf(c))^k \text{ for some integer } k \text{ (} 1 \leq k \leq h). \text{ Then } c(c^{-1}v^{-1}cv) = v^{-1}cv = y^{-1}cy = c^{f(c)}, \text{ so } k = 1, \text{ and } f(c) = c^{-1}v^{-1}cv = f_{v^{-1}}(c). \text{ Hence } f \text{ is a principal crossed homomorphism.}

In the remainder of this paper suppose \( R \) is a (not necessarily commutative) finite local ring with radical \( M \). \text{ Let } R/M = K \cong GF(p^r)(p \text{ a prime).} \text{ Let } |R| = p^{ar}, |M| = p^{(n-1)r}, R^* \text{ the unit group of } R, \text{ and } p^k \text{ the characteristic of } R. \text{ The } r\text{-dimensional Galois extension } GR(p^{kr}, p^k) \text{ of } Z_{p^k} = Z/p^kZ \text{ is called a Galois ring (see [4]). By [5, Theorem 8 (i)]}, \text{ } R \text{ contains a subring isomorphic to } GR(p^{kr}, p^k), \text{ which will be called a maximal Galois subring of } R. \text{ If } R_1 \text{ and } R_2 \text{ are two maximal Galois subrings of } R, \text{ then by [5, Theorem 8 (ii)]}, \text{ there exists } a \in R^* \text{ such that } R_2 = a^{-1}R_1a. \text{ In the proof of [6, Theorem], the author has proved that } R^* \text{ contains an element } u \text{ such that (i) its multiplicative order is } p^r-1, \text{ and (ii) } Z_{p^k}[u], \text{ the subring of } R \text{ generated by } u, \text{ is a maximal Galois subring of } R.

Let \( N = |x \in M| xu = ux| \) be a subgroup of the additive group of \( M \), then, by [6, Remark], the number of maximal Galois subrings of \( R \) is equal to \( |M: N|, \) the index of \( N \) in \( M \). \text{ In the following we fix such an element } u. \text{ Note that, if } u' \text{ is another such element, then } N \text{ and } N' = |x \in M| xu' = u'x| \text{ consist of the same number of elements.}

Let us define \( \phi: \langle u \rangle \to Aut(1+M) \) by \( \phi(x) = v^{-1}xv \) \( (v \in \langle u \rangle, x \in 1+M). \) By Theorem 1 and [7, Theorem 1 (2)], we see that \( |Z_p^\phi(\langle u \rangle, 1+M)|, |B_\phi(\langle u \rangle, 1+M)|, \text{ and } |M: N| \text{ are all equal to the number of maximal Galois subrings of } R. \text{ As } M \text{ and } N \text{ are modules over } Z_{p^k}[u], \text{ by [4, p. 310 Theorem (XVI.2)]}, |M: N| \text{ is a power of } p^r.

We will deal with the equation
\[
(1) \quad X^{p^r-1} = 1
\]
in \( R \).

\textbf{Theorem 2.} \textit{Let } \( N_i = |x \in M| u^i x = xu^i| \text{ be a submodule of } M, \text{ } |M: N_i| \text{ the index of } N_i \text{ in } M, \text{ and } v \text{ the number of solutions of (1) in } R. \text{ Then.}

\[
\nu = \sum_{d \mid p^r-1} \phi(d) |M: N_{(p^r-1)/d}|,
\]

where \( \phi \) is the Euler function.
Proof. In the following, the word "order" always means the multiplicative order.

If \( t \in R^* \) satisfies \( t^{p^r-1} = 1 \), then the order of \( t \) is a divisor of \( p^r - 1 \). When \( d \) is a divisor of \( p^r - 1 \), let \( S_d \) denote the set of all elements in \( R^* \) with order \( d \), then \( \nu = \sum_{d|p^r-1} |S_d| \). Any \( t \in R^* \) is uniquely written as \( t = vx, v \in \langle u \rangle, x \in 1 + M \).

If the order of \( t = vx \ (v \in \langle u \rangle, x \in 1+M) \) is \( d \), then the order of \( v \) is \( d \), for, orders of \( \langle u \rangle \) and \( 1+M \) are coprime. Hence, if \( t = vx \in S_d \), then \( v = u^{hs} \), where \( h = (p^r-1)/d \) and \( s \) is an integer with \( 1 \leq s < d \). \( (s, d) = 1 \). The number of such \( s \)'s is \( \phi(d) \).

Let \( s \) be such an integer and \( t = u^{hs}x \in S_d \ (x \in 1+M) \), then both of \( \langle t \rangle \) and \( \langle u^{hs} \rangle \) are Hall subgroups of \( G = \langle (u^{hs})^j | 1 \leq j \leq d, z \in 1+M \rangle \) with the order \( dp^{(n-1)r} \). So, there exists some \( y \in 1+M \) and an integer \( 1 \leq i < d \) such that \( (i, d) = 1 \) and \( t = y^{-1}(u^{hs})^iy \). Then \( (s, d) = 1 \), so we see that \( S_d = |x^{-1}u^{hs}x| \leq s < d, (s, d) = 1, x \in 1+M| \).

Let us put \( H_s = \{x^{-1}u^{hs}x | x \in 1+M \} \) for each fixed \( u^{hs} \). Since \( x^{-1}u^{hs}x = x^{-1}u^{hs}x' (x, x' \in 1+M) \) is equivalent to \( s = s' \) and \( xx'^{-1} \in N_{hs} \), we have \( |H_s| = |M: N_{hs}| \). When \( (s, d) = 1 \), \( N_{hs} = N_h \), so \( |H_s| = |M: N_h| \). Hence, \( |S_d| = \phi(d) |M: N_h| \) and \( \nu = \sum_{d|p^r-1} |S_d| = \sum_{d|p^r-1} \phi(d) |M: N_{p^r-1/d}| \), which completes the proof.

**Corollary.** If \( r \geq 2 \), then

\[
(p^r - 1) \left[ \left\lfloor \frac{\phi(p^r-1)(|M: N|-1)+p^r-2}{p^r-1} \right\rfloor + 1 \right] \leq \nu \leq \frac{(p^r-p)}{p^r-1} \left[ \frac{(p^r-p)}{p^r-1} |M: N|+p-1 \right],
\]

where \( [a] \) denotes the greatest integer not exceeding \( a \).

**Proof.** When \( d \) is a divisor of \( p - 1 \), \( N_{d(p^r-1/d)} = M \) by [7, Theorem 2(3)], so \( \sum_{d|p^r-1} \phi(d) |M: N_{p^r-1/d}| = \sum_{d|p^r-1} \phi(d) = p - 1 \). Then,

\[
\nu = \sum_{d|p^r-1} \phi(d) |M: N_{p^r-1/d}| = \phi(p^r-1) |M: N| + \sum_{d|p^r-1} \phi(d) |M: N_{p^r-1/d}| + (p-1),
\]

where the second term is a sum with respect to all \( d \) such that \( (*) \) \( d \) is a proper divisor of \( p^r-1 \) and not a divisor of \( p-1 \). Since \( M \supseteq N_{p^r-1/d} \supseteq N \),
T. Sumiyama

\[ \phi(p^r - 1) | M: N| + \sum_{i \neq 1} \phi(d) + (p - 1) \leq \nu \leq (\phi(p^r - 1) + \sum_{i \neq 1} \phi(d)) | M: N| + p - 1. \]

Since

\[ \sum_{d \mid (p^r - 1)} \phi(d) = \sum_{d \mid (p^r - 1)} \phi(d) - \sum_{d \mid (p - 1)} \phi(d) - \phi(p^r - 1) = p^r - p - \phi(p^r - 1), \]

\[ \phi(p^r - 1) | M: N| - 1 + p^r - 1 \leq \nu \leq (p^r - p) | M: N| + p - 1. \]

By [1, p. 137 Theorem 9.1.2], \( \nu \) is a multiple of \( p^r - 1 \), so we get the inequality of Corollary.

In case \( R \) has only one maximal Galois subring, equivalent conditions are given in [7, Theorem 2 (2)].

Let us deal with the case \( R \) has a plenty of maximal Galois subrings.

Suppose \( r \geq 2 \) and \( n \geq 2 \). Let \( V \) be a finite nilpotent ring, and moreover a two-sided vector space with dimension \( n - 1 \) over a finite field \( F \cong GF(p^r) \) which satisfies the following (2)–(6) for any \( a, b \in F \) and any \( x, y \in V \).

(2) \( a(xy) = (ax)y \)

(3) \( (xy)a = x(ya) \)

(4) \( (ax)b = a(xb) \)

(5) \( (xa)y = x(ay) \)

(6) If \( x \neq 0 \), then there exists some \( a \in F \) such that \( ax \neq xa \).

Such \( V \) does exist (see [5, Section 1]).

Let \( F^+ V \) denote the Abelian group direct sum \( F \oplus V \) with multiplication

\[ (a, x)(a', x') = (aa', ax' + xa' + xx'). \]

\( F^+ V \) is a finite local ring with radical \( V' = \langle (0, x) | x \in V \rangle \) and \( (F^+ V) / V' \cong F \). Let \( \zeta \) be a multiplicative generator of \( F \), then \( \zeta' = (\zeta, 0) \) has multiplicative order \( p^r - 1 \), and generates a maximal Galois subring of \( F^+ V \) isomorphic to \( F \). Since \( x = 0 \) is the only element of \( V \) such that \( \zeta x = x \zeta \), \( F^+ V \) has \( |V| = p^{(n-1)r} \) maximal Galois subrings.

Theorem 3. Suppose \( n \geq 2 \). If the number of maximal Galois subrings of \( R \) is the largest, that is, if \( R \) has \( p^{(n-1)r} \) maximal Galois subrings, then \( R \) is isomorphic to \( F^+ V \).
ON COHOMOLOGY OF GROUPS IN FINITE LOCAL RINGS

Proof. Suppose $\text{ch } R = p^k$ and $k \geq 2$. As is shown in [5, pp. 200–201], $\sum_{i=1}^{r} Z_{p^k} u^i$ is a direct sum, hence $\sum_{i=1}^{r} pZ_{p^k} u^i$ is a subset of $N$ consisting of $p^{(k-1)r}$ elements. Then $|M : N| \leq p^{n-1/r}/p^{(k-1)r} \leq p^{n-2r}$, which contradicts the assumption. So we see $\text{ch } R = p$. As $R$ is an algebra over $Z_p$ and $R/M \cong GF(p^n)$ is a separable extension of $Z_p$, by Wedderburn-Malcev theorem [2, p. 491 Theorem 72.19], there exists a subfield $K'$ of $R$ isomorphic to $K = R/M$ and $R = K' \oplus M$ as Abelian groups. $K'$ is a maximal Galois subring of $R$, and $M$ is a two-sided vector space over $K'$. $K'$ contains an element $u'$ with order $p^{r-1}$, then $Z_p[u]$ and $K' = Z_p[u']$ are both maximal Galois subrings of $R$. So, the number of elements of $N' = \{ x \in M \mid u'x = xu' \}$ is equal to $|N| = 1$, that is, $x = 0$ is the only element of $M$ satisfying $u'x = xu'$. $f : R \to K' \oplus M$ defined by $f(a + m) = (a, m)$ ($a \in K'$, $m \in M$) gives an isomorphism of $R$ onto $K' \oplus M$.

Acknowledgement. The author would like to express his indebtedness and gratitude to Prof. K. Motose for his helpful suggestion and valuable comments.

REFERENCES


Aichi Institute of Technology
Yagusa-chô, Toyota 470–03 Japan

(Received December 8, 1985)