Math. J. Okayama Univ. 29 (1987), 77—81

# 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 $\rho$: $H \to Aut(G)$ 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 $\rho$: $H \to Aut(G)$ 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 $\bar{G}$ be the semidirect product of $H$ with $G$ determined by $\rho$. That is, any element $x$ of $\bar{G}$ is uniquely written as $x = at$ with $a \in H$ and $t \in G$, and the multiplication is given by

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

Note that $\rho_b(t) = b^{-1}tb$ in $\bar{G}$.

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

$$(cf(c))^s = c^s\rho_{c^{s-1}}(f(c))\rho_{c^{s-2}}(f(c))\ldots\rho_c(f(c))f(c) = c^s f(c^s)$$

for any integer $s \geq 1$, so the order of $c$ is equal to the order of $cf(c)$. As

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

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

Let $N = \{x \in M \mid xu = ux\}$ 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 $M$. In the following we fix such an element $u$. Note that, if $u'$ is another such element, then $N$ and $N' = \{x \in M \mid xu' = u'x\}$ consist of the same number of elements.

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

We will deal with the equation

$$(1)\quad X^{p^r-1} = 1$$

in $R$.

**Theorem 2.** *Let* $N_i = \{x \in M \mid u^ix = xu^i\}$ *be a submodule of* $M$, $|M: N_i|$ *the index of* $N_i$ *in* $M$, *and* $\nu$ *the number of solutions of* (1) *in* $R$. *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 $G' = \{(u^{hs})^j z \mid 1 \leq j \leq d,\ z \in 1+M\}$ 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 $t = y^{-1}(u^{hs})^i y$. Then $(si, d) = 1$, so we see that $S_d = \{x^{-1}u^{hs}x \mid 1 \leq s < d,\ (s, d) = 1,\ x \in 1+M\}$.

Let us put $H_s = \{x^{-1}u^{hs}x \mid x \in 1+M\}$ 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*

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

*where $[\alpha]$ denotes the greatest integer not exceeding $\alpha$.*

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

$$\begin{aligned}\nu &= \sum_{d|(p^r-1)} \phi(d)|M: N_{(p^r-1)/d}| \\ &= \phi(p^r-1)|M: N| + \sum_{(*)} \phi(d)|M: N_{(p^r-1)/d}| + (p-1),\end{aligned}$$

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 $M \supseteq N_{(p^r-1)/d} \supseteq N$,

$$\phi(p^r-1)\,|M:\ N|+\sum_{(*)}\phi(d)+(p-1)\leq\nu\leq$$
$$(\phi(p^r-1)+\sum_{(*)}\phi(d))\,|M:\ N|+p-1.$$

Since

$$\sum_{(*)}\phi(d)=\sum_{d|(p^r-1)}\phi(d)-\sum_{d|(p-1)}\phi(d)-\phi(p^r-1)$$
$$=p^r-p-\phi(p^r-1),$$
$$\phi(p^r-1)(\,|M:\ N|-1)+p^r-1\leq\nu\leq$$
$$(p^r-p)\,|M:\ N|+p-1.$$

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 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 $F\dot{+}V$ denote the Abelian group direct sum $F\oplus V$ with multiplication

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

$F\dot{+}V$ is a finite local ring with radical $V'=\{(0,\ x)\,|\,x\in V\}$ and $(F\dot{+}V)/V'\cong F$. 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 $F\dot{+}V$ isomorphic to $F$. Since $x=0$ is the only element of $V$ such that $\zeta x=x\zeta$, $F\dot{+}V$ 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 $F\dot{+}V$.*

*Proof.* Suppose $ch\ R = p^k$ 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 $|M: N| \leq p^{(n-1)r}/p^{(k-1)r} \leq p^{(n-2)r}$, which contradicts the assumption. So we see $ch\ R = p$. As $R$ is an algebra over $Z_p$ and $R/M \cong GF(p^r)$ 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 $u'x = xu'$. $f: R \to K' \dot{+} M$ defined by $f(a+m) = (a, m)$ $(a \in K', m \in M)$ gives an isomorphism of $R$ onto $K' \dot{+} M$.

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

## REFERENCES

[1] M. HALL: The Theory of Groups, Macmillan, New York, 1959.
[2] C. W. CURTIS, I. REINER: Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, New York-London-Sydney, 1962.
[3] S. S. MACLANE: Homology, Springer-Verlag, Berlin-Heidelberg-New York, 1963.
[4] B. R. MCDONALD: Finite Rings with Identity, Pure & Appl. Math. Ser. 28, Marcel Dekker, New York, 1974.
[5] R. RAGHAVENDRAN: Finite associative rings, Compositio Math. 21 (1969), 195–229.
[6] T. SUMIYAMA: Note on maximal Galois subrings of finite local rings, Math. J. Okayama Univ. 21 (1979), 31–32.
[7] T. SUMIYAMA: On unit groups of finite local rings, Math. J. Okayama Univ. 23 (1981), 195–198.

AICHI INSTITUTE OF TECHNOLOGY
YAGUSA-CHÔ, TOYOTA 470–03 JAPAN

*(Received December 8, 1985)*