*THEORIE DES NOMBRES*

*BESANCON*

*Années 1989/90-1990/91*

# *H. SUZUKI'S GENERALIZATION OF HILBERT'S TH. 94*

*Katsuya MIYAKE*

# H. SUZUKI'S GENERALIZATION OF HILBERT'S TH.94

Katsuya **MIYAKE**

## 1. INTRODUCTION

Recently, H. Suzuki [S] succeeded in giving a proof to the following theorem and an affirmative answer to a classical problem (cf.e.g. Miyake [M1] ~ [M3] and Jaulent [J]):

**Theorem**. Let k be an algebraic number field of finite degree, and K be an unramified abelian extension of k. Then at least [K:k] ideal classes of k become principal in K.

In case that K/k is cyclic of prime degree, we have Hilbert's Theorem 94 in his celebrated "Zahlbericht" [H]. We also have the principal ideal theorem when K is Hilbert's class field of k. The content of the present theorem has been confirmed in various cases, namely, in case that K/k is cyclic in general and in those cases which Terada's theorem is capable to cover; however, it has also been aware of, by group theoretic examples, that all cases must not have been covered by these (cf.[M3]).

It may be worth mentioning that Suzuki's proof is rather elementary; in fact, it consists of a number of analyses of group rings of a finite abelian group and nothing else.

**Acknowledgement This article was prepared while the author was a visiting member of Equipe de Mathématiques de Besançon, C.N.R.S.- U.A.741, Université de Franche-Comté. He would like to express his heartfelt gratitude to the staffs, especially to Professors J. Cougnard and T. Nguyen Quang Do, for their hospitality.**

## 2. THE TRANSLATION INTO GROUP THEORY BY ARTIN'S RECIPROCITY LAW

Let k and K be as in the theorem, and $\tilde{k}$ and $\tilde{K}$ be their absolute class fields, respectively. Put

$$H = \mathrm{Gal}(\tilde{k}/K),\ A = \mathrm{Gal}(\tilde{k}/K), \text{ and } G = \mathrm{Gal}(K/k) = H/A.$$

Then we have the transfer homomorphism

$$\overline{V}_{H \to A}: H/[H,H] \to A$$

where [H,H] is the commutator subgroup of H which is equal to $Gal(\tilde{K}/\tilde{k})$. Therefore, the quotient group $H/[H,H] = Gal(\tilde{k}/k)$ is isomorphic to the absolute ideal class group Cl(k) of k. The kernel of $\overline{V}_{H \to A}$ corresponds exactly to the subgroup of Cl(k) consisting of those classes whose ideals become principal in K.

It is also known that everything can be reduced to "p-primary parts" for prime factors of |Cl(k)|.

3. **ARTIN'S SPLITTING MODULE**. Through inner automorphisms of H, G acts on A; here we use additive notation for the G-module A. Let $c(g,h) \in A$, $g, h \in G$, be a 2-cocycle belonging to the 2-cohomology class of the group extension

$$1 \to A \to H \to G \to 1.$$

Let $B := \oplus_{g \in G - \{1\}} \mathbb{Z}.b(g)$ be a free abelian group generated by a set of symbols $\{b(g) | g \in G - \{1\}\}$, and put $M := A \oplus B$. Then we have a well-defined action of G on M by setting

$$g.b(h) = b(gh) - b(g) + c(g,h),\ g,h \in G.$$

Since $c(g,h)$ lies in A, we also have an exact sequence of G-modules,

$$0 \to A \to M \to I_G \to 0,$$

with nat: $M \to I_G$ defined by $nat(b(g)) = g-1$, $g \in G$, where $I_G$ is the augmentation ideal of $\mathbb{Z}[G]$.
It is easy to see that the quotient module $M/I_G.M$ is isomorphic to $H/[H,H]$. Let

$$Tr_G : M/I_G.M \to M$$

be the G-homomorphism obtained by multiplication of

$$Tr_G := \Sigma_{g \in G}\, g \in \mathbb{Z}[G].$$

Then it is clear that $Im(Tr_G)$ lies in $Ker(nat) = A$. Hence we have a commutative diagram,

$$\begin{array}{ccccc} H/[H,H] & \xrightarrow{\overline{V}_{H \to A}} & A & \hookrightarrow & H \\ \downarrow\wr & \circlearrowright & \| \text{ identity} & & \\ M/I_G.M & \xrightarrow[Tr_G]{} & A & \hookrightarrow & M. \end{array}$$

In particular, we have

$$|\mathrm{Ker}(\overline{V}_{H\to A})| = |H^{-1}(G,M)|.$$

Our purpose is to show

**(3.1)** the order $|G|$ of $G$ divides $|H^{-1}(G,M)|$.

**4.** **THE FIRST REDUCTION**. Fix a basis $\overline{\eta}_i$, $i = 1,\dots,m'$, of the finite abelian group $M/I_G.M$ ($\cong H/[H,H] \cong Cl(k)$) so that it is a direct product $\Pi_i\langle\overline{\eta}_i\rangle$.

Put $q_i = |\langle\overline{\eta}_i\rangle|$. Take a transversal $\eta_i$ of each $\overline{\eta}_i$ in $M$ and choose $\eta_j \in I_G M$, $j = m'+1,\dots, m$, so that $\eta_1,\dots,\eta_m$ generate whole $M$ over $\mathbb{Z}[G]$. Put $q_j = 1$, $j = m'+1,\dots, m$. Let $\oplus_{i=1}^m \mathbb{Z}[G]$ be a direct sum of $m$ copies of $\mathbb{Z}[G]$ and define a surjective $G$-homomorphism $\rho\colon \oplus^m \mathbb{Z}[G] \to M$ by

$$\rho(e_i) = \eta_i,\ e_i = (0,\dots,0,\overset{i}{1},0,\dots,0) \in \oplus_{i=1}^m \mathbb{Z}[G].$$

We have a commutative diagram of exact sequences with $\varphi = \mathrm{nat}\circ\rho$,

$$\begin{array}{ccccccccc}
0 \to & \mathrm{Ker}\,\varphi & \to & \oplus^m \mathbb{Z}[G] & \xrightarrow{\varphi} & I_G & \to 0 \\
 & \downarrow & & \downarrow\rho & & \| & \\
0 \to & A & \to & M & \to & I_G & \to 0 \\
 & \downarrow & & \downarrow & & & \\
 & 0 & & 0 & & &
\end{array}$$

Since $\varphi$ is a $G$-homomorphism, the image of $Tr_G\colon \oplus^m \mathbb{Z}[G] \to \oplus^m \mathbb{Z}[G]$ lies in $\mathrm{Ker}(\varphi)$. For each $i$, $1 \leq i \leq m$, $\rho(q_i e_i)$ belongs to $I_G.M = \rho(\oplus^m I_G)$; therefore there exists $u_i \in \mathrm{Ker}(\rho)$ such that

$$u_i \equiv q_i.e_i \mod \oplus^m I_G,\ i = 1,\dots,m.$$

Let $U := \langle u_1,\dots,u_m\rangle$ be the $G$-submodule of $M$ which is generated by these $u_i$ over $\mathbb{Z}[G]$. Then $\rho$ induces an isomorphism

$$\rho\colon\ \oplus^m \mathbb{Z}[G]/(U+\oplus^m I_G) \xrightarrow{\sim} M/I_G.M,$$

and maps

$$\mathrm{Ker}(Tr_G\colon \oplus^m \mathbb{Z}[G]/(U+\oplus^m I_G) \to \mathrm{Ker}(\varphi)/U)$$

injectively into

$$\mathrm{Ker}(Tr_G\colon M/I_G.M \to A).$$

Therefore, it is sufficient, for our purpose, to show

**Lemma 1**. Suppose that a surjective G-homomorphism

$$\varphi: \oplus^m \mathbb{Z}[G] \to I_G$$

is given. Let $q_i$, $i = 1,\dots,m$, be positive integers and $U = \langle u_1,\dots,u_m \rangle$ be a $\mathbb{Z}[G]$-submodule of $\mathrm{Ker}(\varphi)$ such that

$$u_i \equiv q_i.e_i \bmod \oplus^m I_G,\ i = 1,\dots,m.$$

Then $|G|$ divides $|H^{-1}(G,W_0)|$ where

$$W_0 := \oplus^m \mathbb{Z}[G]/U.$$

5. **A TINY TRICK**. Put $n = |G|$. It is sufficient to prove Lemma 1 under an additional condition,

**(5.1)** Each $q_i$ is a multiple of $n$ for $i = 1,\dots,m$.

In fact, let $\xi: \oplus^m \mathbb{Z}[G] \to \oplus^m \mathbb{Z}[G]$ be an injective G-homomorphism such that

$$\xi(x) = n.x,\ \ x \in \oplus^m \mathbb{Z}[G].$$

Put $U' := \xi(U)$ and $W_0' := \oplus^m \mathbb{Z}[G]/U'$. Then we have

$$H^{-1}(G,W_0) \simeq H^0(G,U),$$
$$H^{-1}(G,W_0') \simeq H^0(G,U'),$$

and also

$$H^0(G,U) \simeq H^0(G,U')$$

because U and U' are isomorphic. Hence we have

$$H^{-1}(G,W_0) \simeq H^{-1}(G,W_0').$$

For U' in $\oplus^m \mathbb{Z}[G]$, we have the condition (5.1).

The merit of (5.1) is to make the structure of

$${}_n(W_0/I_G.W_0) := \{x \in W_0/I_G.W_0 \mid n.x = 0\}$$

simple enough for us to handle it; under (5.1), this is isomorphic to $\oplus^m \mathbb{Z}/n\mathbb{Z}$, and generated by

$$q_i n^{-1}.\ e_i,\ i = 1,\dots,m.$$

From the congruence, $Tr_G \equiv n \bmod I_G$, it follows that

$$\mathrm{Ker}(Tr_G: W_0/I_G.W_0 \to \mathrm{Ker}(\varphi)/U) \subset {}_n(W_0/I_G.W_0)$$

and

$$\mathrm{Im}\,(Tr_G: {}_nW_0/I_G.W_0\ ) \to \mathrm{Ker}(\varphi)/U) \subset \mathrm{Ker}(\varphi) \cap (U + \oplus^m I_G\ )/U.$$

Hereafter, we <u>assume</u> (5.1).

It should be also noted that we have

$$U \cap \oplus^m I_G = I_G.U;$$

in fact, we easily see this from the facts,

$$U/I_G.U \simeq \oplus^m \mathbb{Z},$$

$$U/\,U \cap \oplus^m I_G \simeq (U + \oplus^m I_G)/\oplus^m I_G \simeq \oplus^m \mathbb{Z},$$

and

$$I_G.U \subset U \cap \oplus^m I_G.$$

**6.** **THE SECOND REDUCTION**. Now put

$$y_i := Tr_G.q_i n^{-1}.e_i - u_i,\ i = 1,\dots,m,$$

and denote the $\mathbb{Z}[G]$-submodule of $\oplus^m\mathbb{Z}[G]$ which is generated by these $y_i$ by $Y$. Then we have

$$Y = \langle y_1,\dots,y_m\rangle \subset \oplus^m I_G \cap \operatorname{Ker}(\varphi)$$

and

$$I_G.Y = I_G.U = U \cap \oplus^m I_G.$$

Therefore, we have a natural isomorphism

$$\begin{aligned}\operatorname{Ker}(\varphi) \cap (U + \oplus^m I_G)/U &\simeq \operatorname{Ker}(\varphi) \cap \oplus^m I_G/U \cap \oplus^m I_G \cap \operatorname{Ker}(\varphi)\\ &= \operatorname{Ker}(\varphi) \cap \oplus^m I_G/\,I_G.Y\end{aligned}$$

because $U$ lies in $\operatorname{Ker}(\varphi)$, and a commutative diagram

$$\begin{array}{ccccc}
{}_n(W_0/I_G.W_0) & \xrightarrow{Tr_G} & \operatorname{Ker}(\varphi) \cap (U + \oplus^m I_G)/U & \longrightarrow & \operatorname{Ker}(\varphi)/U\\
\wr\| & & \uparrow\wr & & \\
 & & \operatorname{Ker}(\varphi) \cap \oplus^m I_G/U \cap \oplus^m I_G & & \\
 & & \hookuparrow & & \\
\oplus^m \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\eta]{} & Y/\,I_G.Y & &
\end{array}$$

where $\eta$ is the homomorphism which maps the i-th generator

$(0,\dots,0,1,0,\dots,0)$ of $\oplus^m\mathbb{Z}/n\mathbb{Z}$ to $y_i$ mod $I_G.Y$, $i = 1,\dots,m$. Since

$$\operatorname{Ker}(Tr_G: W_0/I_G.W_0 \longrightarrow \operatorname{Ker}(\varphi)/U)$$

is isomorphic to $\operatorname{Ker}(\eta)$, it is now sufficient to show

**Lemma 2**. For an m-generated $\mathbb{Z}[G]$-module $Y$ of $\operatorname{Ker}(\varphi) \cap \oplus^m I_G$, the order $|Y/\,I_G.Y|$ divides $n^{m-1}$.

**7.** **THE THIRD REDUCTION**. Our $\mathbb{Z}[G]$-homomorphism $\varphi$ induces an exact sequence,

$$0 \longrightarrow \operatorname{Ker}(\varphi) \cap \oplus^m I_G \longrightarrow \oplus^m I_G \longrightarrow I_G^2 \longrightarrow 0,$$

and then

$$0 \rightarrow (\mathrm{Ker}(\varphi) \cap \oplus^m I_G) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow (\oplus^m I_G) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow I_G^2 \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow 0.$$

Let us naturally consider $I_G \otimes_{\mathbb{Z}} \mathbb{Q}$ a submodule of $\mathbb{Q}[G]$. Put

$$\varepsilon_0 := 1 - 1/n.\,Tr_G.$$

Then $I_G \otimes \mathbb{Q}$ coïncides with the subalgebra $\varepsilon_0.\,\mathbb{Q}[G]$ of $\mathbb{Q}[G]$ because $\varepsilon_0.(g-1) = g-1$ for $g \in G$. Moreover, we have

$$\varepsilon_0^2 = \varepsilon_0 = 1/n.\sum_{g \in G} (1-g),$$

and hence $I_G^2 \otimes \mathbb{Q} = I_G \otimes \mathbb{Q}$. Since representations of G over $\mathbb{Q}$ are completely reducible, the last exact sequence shows that there exists a $\mathbb{Q}[G]$-isomorphism

$$\rho: (\mathrm{Ker}(\varphi) \cap \oplus^m I_G) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} (\oplus^{m-1} I_G) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We fix such a $\rho$ and identify $Y = \langle y_1, \ldots, y_m \rangle$ with $\rho(Y) = \langle \rho(y_1), \ldots, \rho(y_m) \rangle$ for simplicity.

Now we construct a good m-generated $\mathbb{Z}[G]$-submodule

$$Y' := \langle y_1', \ldots, y_m' \rangle$$

of $(\oplus^{m-1} I_G) \otimes \mathbb{Q}$ with a surjective $\mathbb{Z}[G]$-homomorphism $\pi: Y' \rightarrow Y$; then we see that

**(7.1)** $|Y/I_G.Y|$ divides $|Y'/I_G.Y'|$;

hence it is sufficient to show Lemma 2 for $Y'$ in place of $Y$: Since $I_G \otimes \mathbb{Q}$ is a direct sum of (commutative) fields over $\mathbb{Q}$, let F be a simple component of it and $\varepsilon$ be the corresponding idempotent.

We have $F = \varepsilon.(I_G \otimes \mathbb{Q}) = \varepsilon.\,\mathbb{Q}[G]$, $\varepsilon^2 = \varepsilon \in \mathbb{Q}[G]$.

Then $\varepsilon.[(\oplus^{m-1} I_G) \otimes \mathbb{Q}]$ is a vector space over F of dimension m-1. Therefore $\varepsilon.(Y \otimes_{\mathbb{Z}} \mathbb{Q})$ is a subspace of dimension at most m-1. Suppose that

$$\varepsilon.[\langle y_1, \ldots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q}] \neq \varepsilon.(Y \otimes \mathbb{Q})$$

where $\langle y_1, \ldots, y_{m-1} \rangle$ is the (m-1)-generated $\mathbb{Z}[G]$-submodule of Y. Then $\varepsilon.y_1, \ldots, \varepsilon.\,y_{m-1}$ are linearly dependent over F. Therefore, if we choose $N \in \mathbb{N}$, $\neq 0$, so that $N.\varepsilon \in \mathbb{Z}[G]$, and some i, $1 \leq i \leq m-1$, we have

$$\varepsilon.[\langle y_1, \ldots, y_{i-1}, y_i + N.\varepsilon.y_m, y_{i+1}, \ldots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q}] = \varepsilon.(Y \otimes \mathbb{Q}).$$

If necessary, we replace the first m-1 elements of the generators of Y in this manner for every simple component F of $I_G \otimes \mathbb{Q}$. Then we may assume that

$$\langle y_1, \ldots, y_{m-1} \rangle \otimes_{\mathbb{Z}} \mathbb{Q} = Y \otimes \mathbb{Q}$$

for simplicity. Define a $\mathbb{Q}[G]$-homomorphism

$$\pi: (\oplus^{m-1} I_G) \otimes \mathbb{Q} \longrightarrow Y \otimes \mathbb{Q}$$

by setting

$$\pi(\tilde{e}_i) = y_i,\ \tilde{e}_i = (0,\dots,0,\overset{i}{\varepsilon_0},0,\dots,0),\ i = 1,\dots,m-1,$$

and take an element $y \in (\oplus^{m-1} I_G) \otimes \mathbb{Q}$ such that $\pi(y) = y_m$. Then the $\mathbb{Z}[G]$-submodule

$$Y' = \langle \tilde{e}_1,\dots,\tilde{e}_{m-1},y \rangle$$

is the desired one.

Note also that $I_G.Y'$ contains $\oplus^{m-1} I_G$ because we have $\varepsilon_0.(g-1) = g-1$ for $g \in G$.
To analyse $Y'/I_G.Y'$, let

$$pr: (\oplus^{m-1} I_G) \otimes \mathbb{Q} \longrightarrow (\oplus^{m-1} I_G) \otimes \mathbb{Q} / \oplus^{m-1} I_G$$

be the natural projection. We identify the last G-module with

$$(\oplus^{m-1} I_G) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \ \ (\subset (\oplus^{m-1} \mathbb{Z}[G]) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})).$$

Then we have

$$pr(\tilde{e}_i) \equiv 1/n. \sum_{g \in G} (1-g).e_i \equiv (1 - 1/n.Tr_G).e_i \mod \oplus^{m-1} I_G$$

for $i = 1,\dots,m-1$. It is clear that we have

$$g.\, pr(\tilde{e}_i) = pr(\tilde{e}_i),\ \ i = 1,\dots,m,$$

for every $g \in G$. Furthermore, we can easily see, in a straight forward way, that

$$[(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})]^G = \langle pr(\tilde{e}_1),\dots,pr(\tilde{e}_{m-1}) \rangle \simeq \oplus^{m-1} \mathbb{Z}/n\mathbb{Z}.$$

Let $M := \langle pr(y) \rangle$ be the mono-generated $\mathbb{Z}[G]$-submodule of $(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})$. Then we have

$$\begin{aligned}
|Y'/I_G.Y'| &= |(M + \langle pr(\tilde{e}_1),\dots,pr(\tilde{e}_{m-1}) \rangle)/I_G.M| \\
&= |(M + [(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})]^G)/I_G.M| \\
&= |M/I_G.M|.|(M + [(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})]^G)/M| \\
&= |M/I_G.M|.|[(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})]^G| / |M \cap [(\oplus^{m-1} I_G) \otimes (\mathbb{Q}/\mathbb{Z})]^G| \\
&= n^{m-1}.|H^{-1}(G,M)|/|H^0(G,M)|.
\end{aligned}$$

Hence, it is sufficient to show

**Lemma 3**. Let $G$ be a finite abelian group and $M$ be a mono-generated $\mathbb{Z}[G]$-module of finite order. Then the order of $H^{-1}(G,M)$ divides that of $H^0(G,M)$.

**8. THE FINAL STEP**. We give a proof to Lemma 3.

Fix a positive integer r, and consider the group ring $\mathbb{Z}/r\mathbb{Z}[G]$ over the finite ring $\mathbb{Z}/r\mathbb{Z}$. We have a standard perfect pairing

$$\mathbb{Z}/r\mathbb{Z}[G] \times \mathbb{Z}/r\mathbb{Z}[G] \to \mathbb{Q}/\mathbb{Z}$$

by setting

$$(g,h) := 1/r.\ \delta_{g,h}, \quad g,h \in G,$$

where $\delta_{g,h}$ is a Kronecker $\delta$. Let

$$\mathrm{inv}: \mathbb{Z}/r\mathbb{Z}[G] \to \mathbb{Z}/r\mathbb{Z}[G]$$

be an automorphism of the group ring given by

$$\mathrm{inv}(g) = g^{-1}, \quad g \in G.$$

Note that G is abelian.

For a direct sum $\oplus^m \mathbb{Z}/r\mathbb{Z}[G]$, we also have a perfect pairing

$$(w,w') := \sum_{i=1}^{m} (w_i, w'_i)$$

$$w = (w_1,\ldots,w_m),\ w' = (w'_1,\ldots,w'_m) \in \oplus^m \mathbb{Z}/r\mathbb{Z}[G].$$

For the given M of Lemma 3,, take a $\mathbb{Z}/r\mathbb{Z}[G]$-presentation of rank m (say) of its dual $M^\wedge$ for some r and m. Then we have an injective $\mathbb{Z}[G]$-homomorphism

$$i: M \to \oplus^m \mathbb{Z}/r\mathbb{Z}[G]$$

because of the perfect pairing of the last algebra. Take a generator $v = (v_1,\ldots,v_m) \in \oplus^m \mathbb{Z}/r\mathbb{Z}[G]$ of M.

Then for $w = (w_1,\ldots,w_m) \in \oplus^m \mathbb{Z}/r\mathbb{Z}[G]$, and for $a \in \mathbb{Z}[G]$, we have

$$(a.v,w) = 0 \text{ for } \forall\, a \in \mathbb{Z}[G]$$

$$\Leftrightarrow \sum_{i=1}^{m} (a.v_i, w_i) = 0 \text{ for } \forall\, a \in \mathbb{Z}[G]$$

$$\Leftrightarrow \Big(a, \sum_{i=1}^{m} \mathrm{inv}(v_i).w_i\Big) = 0 \quad \forall\, a \in \mathbb{Z}[G]$$

$$\Leftrightarrow \sum_{i=1}^{m} \mathrm{inv}(v_i).w_i = 0.$$

Hence the orthogonal $M^\perp$ of M is given by

$$M^\perp = \mathrm{Ker}(\mathrm{inv}(v).: \oplus^m \mathbb{Z}/r\mathbb{Z}[G] \to \mathbb{Z}/r\mathbb{Z}[G])$$

where inv(v). is the homomorphism defined by

$$\mathrm{inv}(v).w := \sum_{i=1}^{m} \mathrm{inv}(v_i).w_i,$$

$$w = (w_1,\ldots,w_m) \in \oplus^m \mathbb{Z}/r\mathbb{Z}[G].$$

Then we have

$$M^\wedge \simeq \mathrm{Im}(\mathrm{inv}(v).)$$

and

$$(M^G)^\wedge \simeq \mathrm{Im}(\mathrm{inv}(v).)/I_G.\,\mathrm{Im}(\mathrm{inv}(v).).$$

Furthermore, since we have $\mathrm{inv}(I_G) = I_G$, the automorphism $\mathrm{inv}\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$ induces an isomorphism

$$(M^G)^\wedge \simeq \mathrm{Im}(v.)/I_G.\mathrm{Im}(v.)$$

where $v.\colon \oplus^m \mathbb{Z}/r\mathbb{Z}[G] \longrightarrow \mathbb{Z}/r\mathbb{Z}[G]$ is the homomorphism defined in the same way as $\mathrm{inv}(v).$ was. Put $q = |M^G|$. Then we have

$$q = |(M^G)^\wedge| = |\mathrm{Im}(v.)/I_G.\mathrm{Im}(v.)|.$$

Now there exist two matrices $U \in M(m,\mathbb{Z})$ and $J \in M(m,I_G)$ such that

$$v.U = v.J \text{ and } \det(U) = q$$

because

$$\mathrm{Im}(v.) = \langle v_1,\ldots,v_m \rangle = \mathbb{Z}.v_1 + \ldots + \mathbb{Z}.v_m + I_G.I_m(v.)$$

and

$$I_G.I_m(v.) = I_G.v_1 + \ldots + I_G.v_m .$$

Therefore we have

$$\det(U - J).v = 0 \text{ in } \mathbb{Z}/r\mathbb{Z}[G].$$

This implies

$$q.(M/I_G.M) = 0$$

because $\det(U - J) \equiv \det(U) \equiv q \bmod I_G$. Since we have

$$M = \mathbb{Z}[G].v = \mathbb{Z}.v + I_G.M,$$

$M/I_G.M$ is a cyclic group whose order divides $q = |M^G|$.
Furthermore we have

$$|M/\mathrm{Ker}(\mathrm{Tr}_G\colon M \to M)| = |\mathrm{Tr}_G.M|$$

because $|M| < \infty$. Therefore we see

$$|H^0(G,M)| = q/\,|\mathrm{Tr}_G.M| = (q/|M/I_G.M|).\,|M/I_G.M|/|M/\mathrm{Ker}(\mathrm{Tr}_G)|$$
$$= (q/|M/I_G.M|).\,|H^{-1}(G,M)|.$$

Since $q/|M/I_G.M|$ is an integer as was seen above, this proves Lemma 3.

Hence, at the same time, Lemmas 1 and 2 are also proved, and so is our theorem.

## REFERENCES


[H] D. Hilbert. Die Theorie der algebraischen Zahlkörper, Jber. dt. Math.-Ver.4 (1897), 175-546 = Gesam. Abh. I, 63-363.

[J] J.-F. Jaulent. L'état actuel du problème de la capitulation, Séminaire de Théorie des Nombres de Bordeaux, Année 1987-1988- Exposé n° 17.

[M1] K. Miyake. The application of the principal ideal theorem to p-groups, Nagoya Math. Jour. 99 (1985), 73-88.

[M2] ________ . The capitulation problem, Sugaku Exposition 1 (1988), 175-194.

[M3] ________ . Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem and the capitulation problem, Expo. Math. 7 (1989), 289-346.

[S] H. Suzuki. A generalization of Hilbert's Theorem 94, Tokyo Metropolitan Univ. Math. Preprint Series 1990: No.6, Dept. Math., Tokyo Metropolitan Univ., Tokyo, 1990; *to appear* in Nagoya Math. Jour. 121 (1991).



Department of Mathematics
College of General Education
Nagoya University
Nagoya 464-01, Japan