Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 483–507

On the Capitulation Problem

Hiroshi Suzuki

In our previous paper [7], we proved a generalization of Hilbert's Theorem 94 which also contains the Principal Ideal Theorem. However, Tannaka-Terada's Principal Ideal Theorem was not contained in it. The purpose of this paper is to extend the main theorem of [7] in a natural way so that it contains Tannaka-Terada's Principal Ideal Theorem as a special case. Our main theorem (Theorem 1) now contains all of the three capitulation theorems: Hilbert's Theorem 94, the Principal Ideal Theorem and Tannaka-Terada's Principal Ideal Theorem.

Introduction.

For an algebraic number field k of finite degree, we denote the ideal class group of k by Cl_k and the Hilbert class field (namely the maximal unramified abelian extension) of k by H_k. For a Galois extension K of k, we denote its Galois group by $G(K/k)$. For a group G, we denote the commutator subgroup of G by G^c and we write $G^{ab} = G/G^c$. We denote the integral group ring of G by $\mathbb{Z}[G]$, and its augmentation ideal by $I_G = \langle g-1 : g \in G\rangle_{\mathbb{Z}[G]}$. For a finite group G we denote the trace of G by $\mathrm{Tr}_G = \sum_{g\in G} g \in \mathbb{Z}[G]$. For a $\mathbb{Z}[G]$-module M, we denote the submodule consisting of G-invariant elements by

$$M^G = \{m \in M : g \cdot m = m \text{ for all } g \in G\}.$$

In Suzuki[7] we proved the following theorem.

Theorem (old version). *Let K be an unramified abelian extension of an algebraic number field k of finite degree. Then the number of ideal classes of k which become principal in K is divisible by the degree $[K:k]$*

Received October 8, 1998.
Revised December 16, 1998.

of the extension K/k. Namely we have

$$[K : k] \,\Big|\, |\mathrm{Ker}\,(Cl_k \to Cl_K)|,$$

where $i : Cl_k \to Cl_K$ is the homomorphism induced by the inclusion map of corresponding ideal groups.

In the case where K/k is cyclic this theorem is nothing else than Hilbert's Theorem 94 (Hilbert[3]).

Hilbert's Theorem 94. *Let K be an unramified cyclic extension of an algebraic number field k of finite degree. Then the number of ideal classes of k which become principal in K is divisible by the degree $[K : k]$.*

Our old version contains the Principal Ideal Theorem (Furtwängler[2]), that is the case $K = H_k$, because the degree $[H_k : k]$ is equal to the order $|Cl_k|$.

Principal Ideal Theorem. *Every ideal of k becomes principal in H_k.*

The old version, however, does not contain Tannaka-Terada's Principal Ideal Theorem (Terada[8]).

Tannaka-Terada's Principal Ideal Theorem. *Let k be a finite cyclic extension of an algebraic number field k_0 of finite degree and K be the genus field of k/k_0 (the maximal unramified extension of k which is abelian over k_0). Then every $G(k/k_0)$-invariant ideal class of k becomes principal in K.*

The purpose of this paper is to prove the following main theorem.

Theorem 1. *Let k be a finite cyclic extension of an algebraic number field k_0 of finite degree, and let K be an unramified extension of k which is abelian over k_0. Then the number of those $G(k/k_0)$-invariant ideal classes of k which become principal in K is divisible by the degree $[K : k]$ of the extension K/k. Namely*

$$[K : k] \,\Big|\, |\mathrm{Ker}\,(Cl_k \to Cl_K)^{G(k/k_0)}|.$$

Our new theorem obviously contains the old version, that is the case $k = k_0$. Now, suppose that K is the genus field of k/k_0. Then we have $[K : k] = |Cl_k/I_{G(k/k_0)}Cl_k| = |Cl_k^{G(k/k_0)}|$. Therefore our theorem clearly implies

$$Cl_k^{G(k/k_0)} \subset \operatorname{Ker}(Cl_k \to Cl_K).$$

This is Tannaka-Terada's Principal Ideal Theorem. Hence our theorem contains Hilbert's Theorem 94, the Principal Ideal Theorem and Tannaka-Terada's Principal Ideal Theorem.

Tannaka-Terada's Principal Ideal Theorem was generalized for endomorphisms in Miyake[5]. This method gives us an endomorphism version of Theorem 1. (About the history and the fundamental theorems of the capitulation problem see Miyake[6].)

Theorem 2 (endomorphism version). *Let K/k be an unramified abelian extension, and let α be an endomorphism of $G(H_K/k)$ such that $\alpha(G(H_K/K)) \subset G(H_K/K)$ and suppose that α induces the identity map on $G(K/k)$. Then α induces an endomorphism of Cl_k through the isomorphism $Cl_k \cong G(H_K/k)^{ab}$ given by Artin's Reciprocity Law, for which we have*

$$[K : k] \,\Big|\, |\{\mathfrak{a} \in \operatorname{Ker}(Cl_k \to Cl_K); \alpha(\mathfrak{a}) = \mathfrak{a}\}|.$$

To prove Theorems 1 and 2, we consider the group transfer of Galois groups which corresponds to the homomorphism of lifting ideals (Artin[1]):

$$\begin{array}{ccccc} Cl_k & & \longrightarrow & & Cl_K \\ \cong\downarrow & & \circlearrowleft & & \downarrow\cong \\ G(H_k/k) & = & G(H_K/k)^{ab} & \to & G(H_K/K) \end{array}$$

Thus Theorem 2 is equivalent to the following group theoretical version:

Theorem 3 (group theoretical endomorphism version). *Let α be an endomorphism of a finite group H, and N be a normal subgroup of H containing H^c. Assume that $\alpha(N) \subset N$ and that α induces the identity map on $G = H/N$. Then the order of the subgroup*

$$\{hH^c \in \operatorname{Ker} V_{H\to N} : \alpha(h)h^{-1} \in H^c\}$$

of the transfer kernel is divisible by $|G| = [H : N]$. Here $V_{H\to N} : H^{ab} \to N^{ab}$ denotes the group transfer from H to N.

Now we summarize the method of Miyake[5] for the convenience of the reader. Consider the descending series

$$H \supset \alpha(H) \supset \alpha^2(H) \supset \cdots \supset \alpha^r(H) \supset \cdots$$

and take r large enough so that this series becomes stable. Put $H_0 = \alpha^r(H)$, $N_0 = N \cap H_0$ and $N' = \operatorname{Ker} \alpha^r$. Then we can write H and N as α -stable semidirect products $H = H_0 \ltimes N'$ and $N = N_0 \ltimes N'$. In this case, we have

$$\operatorname{Ker}(V_{H_0 \to N_0} : H_0^{ab} \longrightarrow N_0^{ab}) \subset \operatorname{Ker}(V_{H \to N} : H^{ab} \longrightarrow N^{ab}).$$

Moreover, the restriction $\alpha|_{H_0}$ of α to H_0 is an automorphism of H_0. By taking H_0 instead of H, we may assume that α is an automorphism.

Therefore we have only to prove the following group theoretical version of Theorem 1 which is the case of Theorem 3 in which α is an automorphism.

Theorem 4 (group theoretical version). *Let N be a normal subgroup of a finite group H containing the commutator subgroup H^c of H. Suppose that a finite cyclic group A of automorphisms of H is given, and assume that N is stable under A and that A acts trivially on $G = H/N$. Then the order of the A-invariant part of the transfer kernel is divisible by the order $|G|$ of G.*

$$|G| \,\Big|\, |\operatorname{Ker}(V_{H \to N} : H^{ab} \longrightarrow N^{ab})^A|.$$

This theorem contains the group theoretical versions of Hilbert's Theorem 94, the Principal Ideal Theorem and Tannaka-Terada's Principal Ideal Theorem.

Remark 1. If A is a non-cyclic abelian group, then the group theoretical version does not hold in general. For example, take a $\mathbb{Z}[A]$-module M of finite order such that $|M^A| < |M/I_A M|$, and put $H = M$, $N = I_A M$. (More interesting examples of transfer kernels with an action of non-cyclic abelian groups are seen in Miyake[6].)

In Section 1, we reduce Theorem 4 to the property for the divisibility of the order of a cohomology module (Proposition 1). In Sections 2 and 3, we give an annihilation mechanism on $\mathbb{Z}[G \times A]$-modules (Proposition

2) by a careful calculation of determinants in the one-variable polynomial ring $\mathbb{Z}[G][T]$ over $\mathbb{Z}[G]$. In Section 4, we dualize this proposition to obtain Proposition 5. In the final section we translate this annihilation mechanism into a property for the divisibility of the order of a cohomology module by the technique used in Suzuki[7] which may be explained in the following way: "If a natural number annihilates a cyclic group, then the order of the cyclic group divides the natural number". This completes our proof of Proposition 1.

§1. Reduction to module theoretical version.

We do not bother to introduce Artin's splitting module, because we only need its kernel.

Lemma 1. *Let H be a finite group and N be a normal subgroup of H. Put $G = H/N$ and take a free presentation $\pi : F \twoheadrightarrow H$ of H. Then we have a commutative exact diagram*

$$\begin{array}{ccccccccc} 1 & \to & \pi^{-1}(N)^{ab} & \to & F/\pi^{-1}(N)^c & \to & G & \to & 1 \\ & & \big\downarrow{\scriptstyle \bar{\pi}|_{\pi^{-1}(N)^{ab}}} & & \big\downarrow{\scriptstyle \bar{\pi}} & & \| & & \\ 1 & \to & N^{ab} & \to & H/N^c & \to & G & \to & 1. \end{array}$$

Put $R = \mathrm{Ker}\,(\bar{\pi}|_{\pi^{-1}(N)^{ab}} : \pi^{-1}(N)^{ab} \to N^{ab})$. *Then*

$$\mathrm{H}^0(G, R) \cong \mathrm{Ker}\,(V_{H\to N} : H^{ab} \to N^{ab}).$$

(Throughout this paper, cohomology is Tate cohomology of a finite group.)

Proof. Since F^{ab} is $\mathbb{Z}$-torsion free, the multiplication by the order $|G|$,

$$|G|\cdot : F^{ab} \overset{V_{F\to\pi^{-1}(N)}}{\to} \pi^{-1}(N)^{ab} \to F^{ab}$$

is injective. Hence the transfer map

$$V_{F\to\pi^{-1}(N)} : F^{ab} \to \pi^{-1}(N)^{ab}$$

is injective. Note that $\pi^{-1}(N)^{ab}$ is isomorphic to the kernel

$$\mathrm{Ker}\,(\overset{\mathrm{rank}F}{\oplus} \mathbb{Z}[G] \to I_G)$$

of the homomorphism which maps the canonical basis e_j of $\overset{\mathrm{rank}F}{\oplus}\mathbb{Z}[G]$ to $\pi(x_j)-1$ for $j=1,\ldots,\mathrm{rank}\,F$, where x_j are the canonical free generators of F (see Lyndon[4]). Therefore we have

$$\mathrm{H}^0(G,\pi^{-1}(N)^{ab})\cong \mathrm{H}^{-1}(G,I_G)\cong G^{ab}.$$

The group transfer $V_{F\to\pi^{-1}(N)}$ coincides with the homomorphism

$$\pi^{-1}(N)F^c/F^c\to\pi^{-1}(N)^{ab}$$

induced by the trace map

$$\mathrm{Tr}_G:\pi^{-1}(N)^{ab}\to\pi^{-1}(N)^{ab}.$$

Then we easily see

$$\begin{aligned} G^{ab} &\cong V_{F\to\pi^{-1}(N)}(F^{ab})/V_{F\to\pi^{-1}(N)}(\pi^{-1}(N)F^c/F^c) \\ &\cong V_{F\to\pi^{-1}(N)}(F^{ab})/\mathrm{Tr}_G(\pi^{-1}(N)^{ab}) \\ &\subseteqq \mathrm{H}^0(G,\pi^{-1}(N)^{ab}). \end{aligned}$$

Hence the image of $V_{F\to\pi^{-1}(N)}$ must coincide with $(\pi^{-1}(N)^{ab})^G$. From the commutative diagram

$$\begin{tikzcd} F^{ab} \arrow[r, hook, "V_{F\to\pi^{-1}(N)}"] \arrow[d, "\pi^{ab}"'] \arrow[dr, phantom, "\circlearrowright"] & \pi^{-1}(N)^{ab} \arrow[d, "\bar{\pi}|_{\pi^{-1}(N)^{ab}}"] \\ H^{ab} \arrow[r, "V_{H\to N}"'] & N^{ab} \end{tikzcd}$$

we see

$$\begin{aligned} &\mathrm{Ker}\,(V_{H\to N}:H^{ab}\to N^{ab}) \\ \cong\ & V_{F\to\pi^{-1}(N)}(F^{ab})\cap\mathrm{Ker}\,\bar{\pi}|_{\pi^{-1}(N)^{ab}}\ /\ V_{F\to\pi^{-1}(N)}(\mathrm{Ker}\,\pi^{ab}) \\ =\ & R\cap(\pi^{-1}(N)^{ab})^G\ /\ \mathrm{Tr}_G R \\ =\ & R^G/\mathrm{Tr}_G R \\ =\ & \mathrm{H}^0(G,R). \end{aligned}$$

□

Now assume that a finite group A acts on H as automorphisms and that N is an A-subgroup. We take a free presentation in the following manner. Let $U=A\ltimes H$ be the semidirect product of A and H. Then we have a short exact sequence

$$1\to N\to U\to A\ltimes G\to 1.$$

Take a free presentation $p_0 : F_0 \twoheadrightarrow U$ of U; then we have a commutative exact diagram

$$\begin{tikzcd}
1 \arrow[r] & p_0^{-1}(N)^{ab} \arrow[r] \arrow[d, "\bar{p}_0|_{p_0^{-1}(N)^{ab}}"'] & F_0/p_0^{-1}(N)^c \arrow[r] \arrow[d, "\bar{p}_0"'] & A \ltimes G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N^{ab} \arrow[r] & U/N^c \arrow[r] & A \ltimes G \arrow[r] & 1.
\end{tikzcd}$$

Then the subgroup $F = p_0^{-1}(H)$ of F_0 is a free group, and

$$p_0|_F : F \longrightarrow\!\!\!\!\!\rightarrow H$$

is a free presentation of H. Put

$$R = \operatorname{Ker}(\bar{p}_0|_{p_0^{-1}(N)^{ab}} : p_0^{-1}(N)^{ab} \to N^{ab}).$$

Then, by Lemma 1, we have an isomorphism

$$\operatorname{Ker}(V_{H\to N} : H^{ab} \to N^{ab}) \cong \mathrm{H}^0(G, R).$$

By the choice of the free presentation, the commutative diagram

$$\begin{tikzcd}
F^{ab} \arrow[r, hook, "V_{F\to p_0^{-1}(N)}"] \arrow[d, "(p_0|_F)^{ab}"'] \arrow[dr, phantom, "\circlearrowleft"] & p_0^{-1}(N)^{ab} \arrow[d, "\bar{p}_0|_{p_0^{-1}(N)^{ab}}"] \\
H^{ab} \arrow[r, "V_{H\to N}"'] & N^{ab}
\end{tikzcd}$$

in the proof of Lemma 1 is a commutative diagram of $\mathbb{Z}[A]$-homomorphisms. Therefore the above isomorphism is a $\mathbb{Z}[A]$-isomorphism. Hence the A-invariant parts are also isomorphic:

$$\operatorname{Ker}(V_{H\to N} : H^{ab} \to N^{ab})^A \cong \mathrm{H}^0(G, R)^A.$$

Since $|p_0^{-1}(N)^{ab}/R| = |N^{ab}|$ is finite, we have

$$R \otimes_{\mathbb{Z}} \mathbb{Q} = p_0^{-1}(N)^{ab} \otimes_{\mathbb{Z}} \mathbb{Q}$$

where $\mathbb{Q}$ is the rational number field. Since the sequence

$$0 \to p_0^{-1}(N)^{ab} \to \overset{\operatorname{rank} F_0}{\oplus} \mathbb{Z}[A \ltimes G] \to I_{G\times A} \to 0$$

is exact and $\mathbb{Q}[A \ltimes G]$ is a semisimple $\mathbb{Q}$-algebra, we see that

$$R \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\overset{\operatorname{rank} F_0 - 1}{\oplus} \mathbb{Q}[A \ltimes G]) \oplus \mathbb{Q}.$$

It is now clear that Theorem 4 is equivalent to the following proposition.

Proposition 1 (module theoretical version). *Let G be a finite abelian group and A be a finite cyclic group. Let R be a finitely generated $\mathbb{Z}[G \times A]$-module such that $R \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\overset{m}{\oplus} \mathbb{Q}[G \times A]) \oplus \mathbb{Q}$, and suppose that R is $\mathbb{Z}$-torsion free. Then $|G|$ divides $|\mathrm{H}^0(G, R)^A|$.*

The proof of this proposition will be given in Section 5.

§2. $\mathbb{Z}$-torsion free dual annihilation version.

In the next section, we prove the following proposition. This is a module theoretical $\mathbb{Z}$-torsion free dual annihilation version of Proposition 1.

Proposition 2 ($\mathbb{Z}$-torsion free dual annihilation version). *Let G be a finite abelian group and A be a finite cyclic group generated by α. Let M be a finitely generated $\mathbb{Z}[G \times A]$-module such that $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \overset{m}{\oplus} \mathbb{Q}[G \times A]$, and suppose that M is $\mathbb{Z}$-torsion free. Then*

$$|\mathrm{H}^{-1}(G, M)^A| \cdot M^{G \times A} \subset \mathrm{Tr}_G((\alpha - 1)^{-1} I_G M),$$

where $(\alpha - 1)^{-1} I_G M$ is the inverse image of $I_G M$ by the homomorphism $\alpha - 1 : M \to M$ which is multiplication by $\alpha - 1$.

For the proof of this proposition, we need four lemmas.

Lemma 2. *Let the notation and the assumptions be as in Proposition 2. Since $\mathrm{Tr}_G((\alpha - 1)^{-1} I_G M) \cong \overset{m}{\oplus} \mathbb{Z}$, we take $a_1, \ldots, a_m \in (\alpha - 1)^{-1} I_G M$ so that their images by Tr_G form a $\mathbb{Z}$-basis of $\mathrm{Tr}_G((\alpha - 1)^{-1} I_G M)$. Put $M_0 = \langle a_1, \ldots, a_m \rangle_{\mathbb{Z}[G]}$. Then the order of $M \,/\, (I_{G \times A} M + M_0)$ is equal to $|A|^m |\mathrm{H}^{-1}(G, M)^A|$.*

Proof. Note that ${\mathrm{Tr}_G}^{-1}(0) \cap M_0 \subset I_{G \times A} M_0 \subset I_G M$. Hence

$$\begin{aligned}
& \mathrm{H}^{-1}(G, M) \,/\, I_A \mathrm{H}^{-1}(G, M) \\
= \;& {\mathrm{Tr}_G}^{-1}(0) \,/\, (I_A {\mathrm{Tr}_G}^{-1}(0) + I_G M) \\
\cong \;& ({\mathrm{Tr}_G}^{-1}(0) + M_0) \,/\, (I_A {\mathrm{Tr}_G}^{-1}(0) + I_G M + M_0) \\
= \;& ((\alpha - 1)^{-1} I_G M + {\mathrm{Tr}_G}^{-1}(0)) \,/\, (I_A {\mathrm{Tr}_G}^{-1}(0) + I_G M + M_0).
\end{aligned}$$

Now it is clear that the homomorphism given by multiplying $\alpha - 1$ induces an isomorphism of $\mathbb{Z}[G \times A]$-modules of finite order:

$$\begin{aligned} & (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) \,/\, ((\alpha-1)^{-1}I_GM + \mathrm{Tr}_G{}^{-1}(0)) \\ \overset{\alpha-1}{\cong} \;& \mathrm{Tr}_G{}^{-1}(0) \cap I_AM \,/\, (I_AM \cap I_GM + I_A\mathrm{Tr}_G{}^{-1}(0)) \\ \cong \;& (I_AM \cap \mathrm{Tr}_G{}^{-1}(0) + I_GM) \,/\, (I_GM + I_A\mathrm{Tr}_G{}^{-1}(0)). \end{aligned}$$

We have $I_AM \cap (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) \subset I_AM \cap \mathrm{Tr}_G{}^{-1}(0)$, because M is $\mathbb{Z}$-torsion free. Moreover we also have

$$M_0 \cap (I_AM \cap \mathrm{Tr}_G{}^{-1}(0) + I_GM) \subset M_0 \cap \mathrm{Tr}_G{}^{-1}(0) \subset I_{G\times A}M_0 \subset I_GM.$$

Therefore we see

$$\begin{aligned} & I_AM \cap \mathrm{Tr}_G{}^{-1}(0) + I_GM \,/\, I_GM + I_A\mathrm{Tr}_G{}^{-1}(0) \\ \cong \;& I_AM \cap \mathrm{Tr}_G{}^{-1}(0) + I_GM + M_0 \,/\, I_GM + I_A\mathrm{Tr}_G{}^{-1}(0) + M_0 \\ = \;& I_AM \cap (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_GM + M_0 \,/\, I_A\mathrm{Tr}_G{}^{-1}(0) \\ & \quad + I_GM + M_0. \end{aligned}$$

Then we obtain

$$\begin{aligned} & |\mathrm{H}^{-1}(G,M)^A| \\ = \;& |\mathrm{H}^{-1}(G,M) \,/\, I_A\mathrm{H}^{-1}(G,M)| \\ = \;& |(\alpha-1)^{-1}I_GM + \mathrm{Tr}_G{}^{-1}(0) \,/\, I_A\mathrm{Tr}_G{}^{-1}(0) + I_GM + M_0| \\ = \;& |(\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) \,/\, I_AM \cap (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_GM + M_0| \\ = \;& |(\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_AM \,/\, I_{G\times A}M + M_0|. \end{aligned}$$

The homomorphism given by multiplying $(\alpha-1)\mathrm{Tr}_G$ induces an isomorphism

$$\begin{aligned} M \,/\, (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_AM \;&\cong\; I_A\mathrm{Tr}_GM \,/\, I_A^2\mathrm{Tr}_GM \\ &=\; \mathrm{H}^{-1}(A, I_A\mathrm{Tr}_GM). \end{aligned}$$

Since $I_A\mathrm{Tr}_GM$ has a submodule of finite index isomorphic to $\overset{m}{\oplus} I_A$, Herbrand's Lemma shows

$$\begin{aligned} & |\mathrm{H}^{-1}(A, I_A\mathrm{Tr}_GM)| \\ = \;& |\mathrm{H}^{-1}(A, \overset{m}{\oplus} I_A)||\mathrm{H}^0(A, I_A\mathrm{Tr}_GM)| \,/\, |\mathrm{H}^0(A, \overset{m}{\oplus} I_A)| \\ = \;& |\mathrm{H}^{-1}(A, \overset{m}{\oplus} I_A)| = |A|^m. \end{aligned}$$

Thus we finally have

$$\begin{aligned}
& |M \,/\, I_{G\times A}M + M_0| \\
= \;& |M \,/\, (\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_A M| \\
& \quad \cdot |(\alpha-1)^{-1}\mathrm{Tr}_G{}^{-1}(0) + I_A M \,/\, I_{G\times A}M + M_0| \\
= \;& |A|^m |\mathrm{H}^{-1}(G,M)^A|.
\end{aligned}$$

□

Lemma 3. *Let G and A be as in Proposition 2. Let M be a $\mathbb{Z}[G\times A]$-module such that $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \overset{m}{\oplus}\mathbb{Q}[G\times A]$ for some $m > 0$ and take a set of generators $w_1, \dots, w_{m+n}$. Let (w_i) be the column vector and put $w = (w_i)$. Assume that a square matrix $Q = (q_{ij}) \in \mathrm{M}(m+n, \mathbb{Z}[G\times A])$, that is, Q is of size $(m+n)\times(m+n)$ with entries in $\mathbb{Z}[G\times A]$, satisfies $Q\cdot w = 0$. Then all the minors of Q of size greater than n are zero.*

Proof. Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Q}[G\times A]$, then the localization $\mathbb{Q}[G\times A]_{\mathfrak{q}}$ at $\mathfrak{q}$ is a field. Since $M\otimes_{\mathbb{Z}}\mathbb{Q} \cong \overset{m}{\oplus}\mathbb{Q}[G\times A]$, $(M\otimes_{\mathbb{Z}}\mathbb{Q})_{\mathfrak{q}}$ is a linear space of dimension m over $\mathbb{Q}[G\times A]_{\mathfrak{q}}$. Because $Qw = 0$ and $w_1, \dots w_{m+n}$ spans $(M\otimes_{\mathbb{Z}}\mathbb{Q})_{\mathfrak{q}}$, the rank of Q at $\mathfrak{q}$ is at most n. Thus all the minors of Q of size greater than n are zero at all prime $\mathfrak{q}$ of $\mathbb{Q}[G\times A]$. Therefore all the minors of Q of size greater than n are zero in $\mathbb{Z}[G\times A]$. The lemma is proved. □

Let $\mathbb{Z}[G][T]$ be the polynomial ring in T over the group ring $\mathbb{Z}[G]$, and let $p : \mathbb{Z}[G][T] \twoheadrightarrow \mathbb{Z}[G\times A]$ be a surjective homomorphism of $\mathbb{Z}[G]$-algebras given by $p(T) = \alpha - 1$. Note that $\mathrm{Ker}\, p = \langle (T+1)^{|A|} - 1\rangle_{\mathbb{Z}[G][T]}$. Write $(T+1)^{|A|} - 1 = T\cdot f(T)$. For a matrix, by abuse of notation, we denote the homomorphism obtained by applying p to every entry also by p.

Lemma 4. *Let S be a noetherian ring, x be an element of S such that x is not a zero divisor and (x) is equal to its radical. Let Q be an $m+n$ square matrix such that Q modulo $\mathfrak{p}$ has at most rank n at every minimal prime $\mathfrak{p}$ of (x). Then x^m divides* $\det(Q)$.

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the minimal primes of (x). Since the radical of (x) is equal to (x), $(x) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$, and $xS_{\mathfrak{p}_j} = \mathfrak{p}_j S_{\mathfrak{p}_j}$. Because the rank of Q mod $\mathfrak{p}_j$ is at most n, $\det Q$ is contained in the m-th power

$x^m S_{\mathfrak{p}_j}$ of the maximal ideal $xS_{\mathfrak{p}_j}$ for all $\mathfrak{p}_j$. Then $\det Q$ is contained in $x^m U^{-1}S$, where $U = S \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s)$ and $U^{-1}S$ is the localization of S by U. Therefore $f \det(Q) \in (x^m)$ for some $f \in U$. Now f is in no minimal prime over (x), so the multiplication by f is injective on $S/(x)$. Since x is not a zero divisor, the multiplication by x^l induces an isomorphism $S/(x) \cong (x^l)/(x^{l+1})$ for every l. The multiplication by f is injective on $(x^l)/(x^{l+1})$ and also on $S/(x^l)$ for all l. Thus $\det(Q) \in (x^m)$ as claimed. □

Remark 2. Let G, A, M, w and Q be as in Lemma 3. Take a matrix $\tilde{Q} = (\tilde{q}_{ij}) \in \mathrm{M}(m+n, \mathbb{Z}[G][T])$ such that $p(\tilde{Q}) = Q$. Then putting $S = \mathbb{Z}[G][T]$ and $x = (T+1)^{|A|} - 1$ in Lemma 4, we have

$$((T+1)^{|A|} - 1)^m \;\Big|\; \det \tilde{Q}.$$

Furthermore all the cofactors of $\tilde{Q}$ are divisible by $((T+1)^{|A|} - 1)^{m-1}$.

For $x \in \mathbb{Z}[G][T]$, define $x^{(<l)}$ and $x^{(\geqq l)} \in \mathbb{Z}[G][T]$ by

$$x = x^{(<l)} + T^l x^{(\geqq l)} \quad \text{with} \quad \deg_T x^{(<l)} < l,$$

and denote the coefficient of T^l by $x^{(l)} \in \mathbb{Z}[G]$. For a matrix, we extend this definition to the whole matrix if it applies to all the entries. Denote the natural projection by

$$pr : \mathbb{Z}[G \times A] \twoheadrightarrow \mathbb{Z}[G \times A]/\langle \alpha - 1 \rangle_{\mathbb{Z}[G \times A]} \cong \mathbb{Z}[G];$$

then $x^{(0)}$ is the image of x by $pr \circ p$.

Remark 3. Under the hypotheses of Remark 2, we have

$$\begin{aligned}
\begin{vmatrix} \tilde{q}^{(0)}_{i_1 j_1} & \cdots & \tilde{q}^{(0)}_{i_1 j_s} \\ \vdots & \ddots & \vdots \\ \tilde{q}^{(0)}_{i_s j_1} & \cdots & \tilde{q}^{(0)}_{i_s j_s} \end{vmatrix}
&= pr \circ p \left(\begin{vmatrix} \tilde{q}_{i_1 j_1} & \cdots & \tilde{q}_{i_1 j_s} \\ \vdots & \ddots & \vdots \\ \tilde{q}_{i_s j_1} & \cdots & \tilde{q}_{i_s j_s} \end{vmatrix} \right) \\
&= pr \left(\begin{vmatrix} q_{i_1 j_1} & \cdots & q_{i_1 j_s} \\ \vdots & \ddots & \vdots \\ q_{i_s j_1} & \cdots & q_{i_s j_s} \end{vmatrix} \right) = 0 \qquad \text{for } s > n.
\end{aligned}$$

Lemma 5. *Under the hypotheses of Remark 2, we have*

$$(\det\tilde{Q})^{(\geqq m)}\cdot E=(\operatorname{adj}\tilde{Q})^{(m-1)}\tilde{Q}^{(\geqq 1)}+(\operatorname{adj}\tilde{Q})^{(\geqq m)}\tilde{Q},$$

where E is the unit matrix and $\operatorname{adj}\tilde{Q}$ *is the cofactor matrix of $\tilde{Q}$.*

Proof. Since the cofactor matrix $\operatorname{adj}\tilde{Q}$ is divisible by T^{m-1}, we have

$$\begin{aligned}
&\det\tilde{Q}\cdot E\\
=\;&\operatorname{adj}\tilde{Q}\cdot\tilde{Q}\\
=\;&T^{m-1}(\operatorname{adj}\tilde{Q})^{(\geqq m-1)}\cdot\tilde{Q}\\
=\;&T^{m-1}(\operatorname{adj}\tilde{Q})^{(m-1)}\cdot T\tilde{Q}^{(\geqq 1)}+T^{m-1}(\operatorname{adj}\tilde{Q})^{(m-1)}\tilde{Q}^{(0)}\\
&\quad+T^{m}(\operatorname{adj}\tilde{Q})^{(\geqq m)}\tilde{Q}\\
=\;&T^{m}((\operatorname{adj}\tilde{Q})^{(m-1)}\tilde{Q}^{(\geqq 1)}+(\operatorname{adj}\tilde{Q})^{(\geqq m)}\tilde{Q})\\
&\quad+T^{m-1}(\operatorname{adj}\tilde{Q})^{(m-1)}\tilde{Q}^{(0)}.
\end{aligned}$$

Since $\det\tilde{Q}$ is divisible by T^m, $(\operatorname{adj}\tilde{Q})^{(m-1)}\tilde{Q}^{(0)}$ must be equal to zero. This proves the lemma. □

§3. Proof of Proposition 2.

We may assume $m>0$. Take $a_1,\dots,a_m\in(\alpha-1)^{-1}I_GM$ as in Lemma 2, and put

$$M_0=\langle a_1,\dots,a_m\rangle_{\mathbb{Z}[G\times A]}.$$

Take $b_1,\dots,b_n\in M$ so that $b_1,\dots,b_n,a_1,\dots,a_m$ generate M. Put

$$a=\begin{pmatrix}a_1\\ \vdots\\ a_m\end{pmatrix},\ b=\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}\ \text{ and } v=\begin{pmatrix}b\\ a\end{pmatrix}.$$

Then by Lemma 2, we find a square matrix $B\in\mathrm{M}(n,\mathbb{Z})$ such that $Bb\in\overset{m+n}{\oplus}(I_{G\times A}M+M_0)$ and

$$\det B=|M\,/\,I_{G\times A}M+M_0|=|A|^m|\mathrm{H}^{-1}(G,M)^A|.$$

There exist matrices $J_1\in\mathrm{M}(n,I_{G\times A})$ and $L\in\mathrm{M}(n,m,\mathbb{Z}[G\times A])$ such that $Bb=J_1b+La$. Since $(\alpha-1)M_0\subset I_GM$, there exist $J_2\in$

$\mathrm{M}(m, \langle I_G\rangle_{\mathbb{Z}[G\times A]})$ and $J_3 \in \mathrm{M}(m, n, \langle I_G\rangle_{\mathbb{Z}[G\times A]})$ such that $(\alpha - 1)a = J_2 a + J_3 b$. Put

$$X = \begin{pmatrix} B - J_1 & -L \\ -J_3 & (\alpha - 1)E - J_2 \end{pmatrix} \in \mathrm{M}(m+n, \mathbb{Z}[G \times A]).$$

Then $X \cdot v = 0$. Write $X = (x_{ij})$.

Now take a lift $\tilde{J}_1 \in \mathrm{M}(n, \langle I_G, T\rangle_{\mathbb{Z}[G][T]})$, $\tilde{L} \in \mathrm{M}(n, m, \mathbb{Z}[G][T])$, $\tilde{J}_2 \in \mathrm{M}(m, \langle I_G\rangle_{\mathbb{Z}[G][T]})$ and $\tilde{J}_3 \in \mathrm{M}(m, n, \langle I_G\rangle_{\mathbb{Z}[G][T]})$ of J_1, L, J_2 and J_3 under the map p, respectively. Put

$$\tilde{X} = \begin{pmatrix} B - \tilde{J}_1 & -\tilde{L} \\ -\tilde{J}_3 & TE - \tilde{J}_2 \end{pmatrix}$$

and write $\tilde{X} = (\tilde{x}_{ij})$. Then $\tilde{X}$ is a lift of X under p. By Remark 2, $\det \tilde{X}$ is divisible by $((T+1)^{|A|} - 1)^m$. Put $\tilde{D} = (\det \tilde{X})^{(\geqq m)}$. Then by Lemma 5,

$$\tilde{D} \cdot E = (\operatorname{adj} \tilde{X})^{(m-1)} \tilde{X}^{(\geqq 1)} + (\operatorname{adj} \tilde{X})^{(\geqq m)} \tilde{X}.$$

Note that $\tilde{D}$ is divisible by $f(T)^m$ and that

$$\tilde{D} \equiv \det B \equiv |A|^m |\mathrm{H}^{-1}(G, M)^A| \mod \langle I_G, T\rangle_{\mathbb{Z}[G][T]}.$$

Take an element $c = (c_1, \ldots, c_{m+n})$ of $\overset{m+n}{\oplus} \mathbb{Z}[G \times A]$ such that $c \cdot v \in M^{G\times A}$, and take a lift $\tilde{c} = (\tilde{c}_1, \ldots, \tilde{c}_{m+n}) \in \overset{m+n}{\oplus} \mathbb{Z}[G][T]$ of c. Put

$$D_1 = \begin{vmatrix} \tilde{c}_1^{(0)} & \cdots & \tilde{c}_{m+n}^{(0)} \\ \tilde{x}_{2\,1} & \cdots & \tilde{x}_{2\,m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\,1} & \cdots & \tilde{x}_{m+n\,m+n} \end{vmatrix}^{(m-1)},$$

$\ldots,$

$$D_{m+n} = \begin{vmatrix} \tilde{x}_{1\,1} & \cdots & \tilde{x}_{1\,m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n-1\,1} & \cdots & \tilde{x}_{m+n-1\,m+n} \\ \tilde{c}_1^{(0)} & \cdots & \tilde{c}_{m+n}^{(0)} \end{vmatrix}^{(m-1)} \in \mathbb{Z}[G].$$

Then we see that

$$
\begin{aligned}
&\tilde{D}\tilde{c} \\
= \ & \tilde{c}\tilde{D}E \\
= \ & \tilde{c}^{(0)}\tilde{D}E + T\tilde{c}^{(\geqq 1)}\tilde{D}E \\
= \ & \tilde{c}^{(0)}(\operatorname{adj}\tilde{X})^{(m-1)}\tilde{X}^{(\geqq 1)} + \tilde{c}^{(0)}(\operatorname{adj}\tilde{X})^{(\geqq m)}\tilde{X} + T\tilde{c}^{(\geqq 1)}\tilde{D}E \\
= \ & (D_1, \cdots, D_{m+n}) \cdot \begin{pmatrix} -\tilde{J}_1^{(\geqq 1)} & -\tilde{L}_1^{(\geqq 1)} \\ -\tilde{J}_3^{(\geqq 1)} & E - \tilde{J}_2^{(\geqq 1)} \end{pmatrix} \\
& \quad + \tilde{c}^{(0)}(\operatorname{adj}\tilde{X})^{(\geqq m)}\tilde{X} \\
& \quad + T\tilde{c}^{(\geqq 1)}\tilde{D}E.
\end{aligned}
$$

We have

$$
\begin{pmatrix}
x_{1\ 1} & \cdots & x_{1\ m+n} \\
\vdots & & \vdots \\
(\alpha-1)c_1 & \cdots & (\alpha-1)c_{m+n} \\
\vdots & & \vdots \\
x_{m+n\ 1} & \cdots & x_{m+n\ m+n}
\end{pmatrix} v = 0.
$$

Therefore the determinant

$$
\begin{vmatrix}
\tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\
\vdots & & \vdots \\
T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\
\vdots & & \vdots \\
\tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n}
\end{vmatrix}
$$

is divisible by $((T+1)^{|A|}-1)^m$, and hence

$$
\begin{vmatrix}
\tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\
\vdots & & \vdots \\
T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\
\vdots & & \vdots \\
\tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n}
\end{vmatrix}^{(\geqq m)}
$$

is divisible by $f(T)^m$. By Remark 3, we have

$$D_i = \left| \left| \begin{matrix} \tilde{x}_{1\,1} & \cdots & \tilde{x}_{1\,m+n} \\ \vdots & & \vdots \\ T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\,1} & \cdots & \tilde{x}_{m+n\,m+n} \end{matrix} \right|^{(\geqq m)} \right|_{T=0}.$$

In fact,

$$\begin{aligned} D_i &= \left| \begin{matrix} \tilde{x}_{1\,1} & \cdots & \tilde{x}_{1\,m+n} \\ \vdots & & \vdots \\ \tilde{c}_1^{(0)} & \cdots & \tilde{c}_{m+n}^{(0)} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\,1} & \cdots & \tilde{x}_{m+n\,m+n} \end{matrix} \right|^{(m-1)} \\ &= \left| \begin{matrix} \tilde{x}_{1\,1} & \cdots & \tilde{x}_{1\,m+n} \\ \vdots & & \vdots \\ T\tilde{c}_1^{(0)} & \cdots & T\tilde{c}_{m+n}^{(0)} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\,1} & \cdots & \tilde{x}_{m+n\,m+n} \end{matrix} \right|^{(m)} \\ &= \left| \begin{matrix} \tilde{x}_{1\,1} & \cdots & \tilde{x}_{1\,m+n} \\ \vdots & & \vdots \\ T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\,1} & \cdots & \tilde{x}_{m+n\,m+n} \end{matrix} \right|^{(m)} \\ &\qquad - \sum \pm \left| \begin{matrix} \tilde{x}_{i_1 j_1}^{(0)} & \cdots & \tilde{x}_{i_1 j_s}^{(0)} \\ \vdots & \ddots & \vdots \\ \tilde{x}_{i_s j_1}^{(0)} & \cdots & \tilde{x}_{i_s j_s}^{(0)} \end{matrix} \right| \tilde{c}_{l_1}^{(t_1)} \tilde{x}_{k_2 l_2}^{(t_2)} \cdots \tilde{x}_{k_r l_r}^{(t_r)}. \end{aligned}$$

Here $\sum$ is taken over all $t_1, \ldots, t_r > 0$ with $t_1 + \cdots + t_r = m-1$, all $1 \leqq k_2 < \cdots < k_r \leqq m+n$ except i and all distinct $1 \leqq l_1, \ldots, l_r \leqq m+n$. The indices $1 \leqq i_1 < \ldots < i_s \leqq m+n$ are taken as $\{i_1, \ldots, i_s\} = \{1, \ldots, m+n\} \setminus \{i, k_2, \ldots, k_r\}$, and $1 \leqq j_1 < \ldots < j_s \leqq m+n$ are taken as $\{j_1, \ldots, j_s\} = \{1, \ldots, m+n\} \setminus \{l_1, \ldots, l_r\}$. Since $r \leqq t_1 + \cdots + t_r = m-1$, we see that $s = m+n-r > n$. Therefore by Remark 3, all of the terms in $\sum$ vanish. Hence we have

$$
\begin{aligned}
D_i &= \begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}^{(m)} \\
&= \left. \begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ T\tilde{c}_1 & \cdots & T\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}^{(\geqq m)} \right|_{T=0} .
\end{aligned}
$$

Thus D_i is divisible by $f(0)^m = |A|^m$. Moreover since

$$
\begin{pmatrix} x_{1\ 1} & \cdots & x_{1\ m+n} \\ \vdots & & \vdots \\ (g-1)c_1 & \cdots & (g-1)c_{m+n} \\ \vdots & & \vdots \\ x_{m+n\ 1} & \cdots & x_{m+n\ m+n} \end{pmatrix} v = 0 \quad (g \in G),
$$

a similar argument to the above also implies

$$
\begin{aligned}
&(g-1)D_i \\
&= \begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ (g-1)\tilde{c}_1^{(0)} & \cdots & (g-1)\tilde{c}_{m+n}^{(0)} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}^{(m-1)} \\
&= \begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ (g-1)\tilde{c}_1 & \cdots & (g-1)\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}^{(m-1)} \\
&\quad -\sum \pm \begin{vmatrix} \tilde{x}_{i_1 j_1}^{(0)} & \cdots & \tilde{x}_{i_1 j_s}^{(0)} \\ \vdots & \ddots & \vdots \\ \tilde{x}_{i_s j_1}^{(0)} & \cdots & \tilde{x}_{i_s j_s}^{(0)} \end{vmatrix} (g-1)\tilde{c}_{l_1}^{(t_1)} \tilde{x}_{k_2 l_2}^{(t_2)} \cdots \tilde{x}_{k_r l_r}^{(t_r)} \\
&= \begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ (g-1)\tilde{c}_1 & \cdots & (g-1)\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}^{(m-1)} .
\end{aligned}
$$

($\sum$ is again taken over all $t_1, \dots, t_r > 0$ with $t_1 + \cdots + t_r = m-1$, all $1 \leqq k_2 < \cdots < k_r \leqq m+n$ except i and all distinct $1 \leqq l_1, \dots, l_r \leqq m+n$. The indices $1 \leqq i_1 < \ldots < i_s \leqq m+n$ are taken as $\{i_1, \dots, i_s\} = \{1, \dots, m+n\} \setminus \{i, k_2, \dots, k_r\}$, and $1 \leqq j_1 < \ldots < j_s \leqq m+n$ are taken as $\{j_1, \dots, j_s\} = \{1, \dots, m+n\} \setminus \{l_1, \dots, l_r\}$.) By Remark 2, we have that

$$
\begin{vmatrix} \tilde{x}_{1\ 1} & \cdots & \tilde{x}_{1\ m+n} \\ \vdots & & \vdots \\ (g-1)\tilde{c}_1 & \cdots & (g-1)\tilde{c}_{m+n} \\ \vdots & & \vdots \\ \tilde{x}_{m+n\ 1} & \cdots & \tilde{x}_{m+n\ m+n} \end{vmatrix}
$$

is divisible by T^m. Therefore the coefficient of T^{m-1} in the determinant is equal to zero. Thus we conclude that $(g-1)D_i$ are zero for all $g \in G$. Hence

$$D_1, \dots, D_{m+n} \in |A|^m \mathbb{Z}[G] \cap \mathbb{Z}\mathrm{Tr}_G = |A|^m \mathbb{Z}\mathrm{Tr}_G.$$

Since we have

$$\tilde{X} = \begin{pmatrix} B - \tilde{J}_1 & -\tilde{L} \\ -\tilde{J}_3 & TE - \tilde{J}_2 \end{pmatrix} \equiv \begin{pmatrix} B - \tilde{J}_1 & -\tilde{L} \\ O & TE \end{pmatrix} \mod \langle I_G \rangle_{\mathbb{Z}[G][T]},$$

each D_i is congruent to zero modulo I_G and hence equal to zero for $1 \leqq i \leqq n$. Take $h_k \in \mathbb{Z}$ such that $D_{n+k} = h_k |A|^m \mathrm{Tr}_G$ for $k = 1, \dots, m$. Now put $D = p(\tilde{D}) = p(\det \tilde{X}^{(\geqq m)})$. Then $f(T)^m$ divides $\tilde{D}$. Since $(\alpha - 1) f(\alpha - 1) = 0$, $(\alpha - 1)D$ is equal to zero. Moreover $X \cdot v = 0$. Therefore

$$\begin{aligned} & D \cdot cv \\ = \; & p(\tilde{D}\tilde{c})v \\ = \; & (0, \dots, 0, D_{n+1}, \dots, D_{m+n})\, p(\tilde{X}^{(\geqq 1)})v \\ = \; & (0, \dots, 0, h_1, \dots, h_m)|A|^m \mathrm{Tr}_G\, p(\tilde{X}^{(\geqq 1)})v. \end{aligned}$$

Since we have

$$\tilde{X}^{(\geqq 1)} \equiv \begin{pmatrix} -\tilde{J}_1^{(\geqq 1)} & -\tilde{L}^{(\geqq 1)} \\ O & E \end{pmatrix} \mod \langle I_G \rangle_{\mathbb{Z}[G][T]},$$

we see that

$$\begin{aligned} D \cdot cv &= h_1 |A|^m \mathrm{Tr}_G a_1 + \cdots + h_m |A|^m \mathrm{Tr}_G a_m \\ &\in |A|^m \mathrm{Tr}_G((\alpha - 1)^{-1} I_G M). \end{aligned}$$

This is true for every $cv \in M^{G \times A}$. Since $D \equiv |A|^m |\mathrm{H}^{-1}(G, M)^A|$ mod $I_{G \times A}$ and since $c \cdot v$ runs through all the elements of $M^{G \times A}$, we see that

$$|A|^m \cdot |\mathrm{H}^{-1}(G, M)^A| M^{G \times A} \subset |A|^m \cdot \mathrm{Tr}_G((\alpha - 1)^{-1} I_G M).$$

By assumption M is $\mathbb{Z}$-torsion free. Therefore we conclude

$$|\mathrm{H}^{-1}(G, M)^A| M^{G \times A} \subset \mathrm{Tr}_G((\alpha - 1)^{-1} I_G M).$$

Proposition 2 is now proved.

§4. Dualization of Proposition 2.

In this section, we dualize Proposition 2 through the intermediary of finite modules.

Proposition 3 (finite dual annihilation version). *Let G be a finite abelian group and A be a finite cyclic group generated by α. For a $\mathbb{Z}[G\times A]$-module M of finite order, we have*

$$|\mathrm{H}^{-1}(G,M)^A|\cdot M^{G\times A}\subset \mathrm{Tr}_G((\alpha-1)^{-1}I_GM).$$

Proof. Let s be the exponent of M and denote the Pontrjagin dual of M by $M^\wedge$. Take a sufficiently large natural number m and take a surjective homomorphism

$$q:\overset{m}{\oplus}\mathbb{Z}/s\mathbb{Z}[G\times A]\twoheadrightarrow M^\wedge.$$

Then, since $\mathbb{Z}/s\mathbb{Z}[G\times A]^\wedge\cong\mathbb{Z}/s\mathbb{Z}[G\times A]$, we have an injective homomorphism

$$i:M\hookrightarrow\overset{m}{\oplus}\mathbb{Z}/s\mathbb{Z}[G\times A].$$

Let us consider M as a submodule of $\overset{m}{\oplus}\mathbb{Z}/s\mathbb{Z}[G\times A]$. Let R be the inverse image of M by the natural projection $p:\overset{m}{\oplus}\mathbb{Z}[G\times A]\twoheadrightarrow\overset{m}{\oplus}\mathbb{Z}/s\mathbb{Z}[G\times A]$. The kernel of p is isomorphic to $\overset{m}{\oplus}\mathbb{Z}[G\times A]$. Therefore we have an exact sequence

$$0\to\overset{m}{\oplus}\mathbb{Z}[G\times A]\to R\to M\to 0.$$

Then $\mathrm{H}^{-1}(G,R)\cong\mathrm{H}^{-1}(G,M)$ as $\mathbb{Z}[A]$-modules and

$$\mathrm{H}^{-1}(G,R)^A\cong\mathrm{H}^{-1}(G,M)^A.$$

Moreover, we have

$$\mathrm{H}^0(G\times A,R)\cong\mathrm{H}^0(G\times A,M).$$

The exact sequence given above induces an exact sequence

$$0\to\overset{m}{\oplus}\mathbb{Z}[G\times A]/\overset{m}{\oplus}\mathbb{Z}[G\times A]\cap I_GR\to R/I_GR\to M/I_GM\to 0.$$

It is clear that

$$\begin{aligned} I_G \cdot \overset{m}{\oplus}\mathbb{Z}[G\times A] &\subset \overset{m}{\oplus}\mathbb{Z}[G\times A]\cap I_G R \\ &\subset \overset{m}{\oplus}\mathbb{Z}[G\times A]\cap {\mathrm{Tr}_G}^{-1}(0) \\ &\subset I_G \cdot \overset{m}{\oplus}\mathbb{Z}[G\times A]. \end{aligned}$$

Therefore the term $\overset{m}{\oplus}\mathbb{Z}[G\times A]/\overset{m}{\oplus}\mathbb{Z}[G\times A]\cap I_G R$ in the previous exact sequence is isomorphic to the free $\mathbb{Z}[A]$-module $\overset{m}{\oplus}\mathbb{Z}[A]$. Thus the homomorphism $R/I_G R \to M/I_G M$ induced by $R \to M$ induces the isomorphism

$$\mathrm{H}^0(A, R/I_G R) \cong \mathrm{H}^0(A, M/I_G M).$$

It is easy to see that

$$\begin{aligned} & R^{G\times A}/\mathrm{Tr}_G((\alpha-1)^{-1}I_G R) \\ \cong\ & \mathrm{Cok}\,(\mathrm{Tr}_G : \mathrm{H}^0(A, R/I_G R) \to \mathrm{H}^0(G\times A, R)) \end{aligned}$$

and

$$\begin{aligned} & M^{G\times A}/\mathrm{Tr}_G((\alpha-1)^{-1}I_G M) \\ \cong\ & \mathrm{Cok}\,(\mathrm{Tr}_G : \mathrm{H}^0(A, M/I_G M) \to \mathrm{H}^0(G\times A, M)). \end{aligned}$$

Hence we have

$$R^{G\times A}\ /\ \mathrm{Tr}_G((\alpha-1)^{-1}I_G R) \cong M^{G\times A}\ /\ \mathrm{Tr}_G((\alpha-1)^{-1}I_G M).$$

Proposition 2 for R now gives Proposition 3 for M. □

Next we take the Pontrjagin dual of the preceding proposition.

Proposition 4 (finite annihilation version). *Let G be a finite abelian group and A be a finite cyclic group. Let M be a $\mathbb{Z}[G\times A]$-module of finite order. Then*

$$|\mathrm{H}^0(G, M)^A| \cdot {\mathrm{Tr}_G}^{-1}(I_A \cdot M^G) \subset I_{G\times A}M.$$

Proof. Take the Pontrjagin dual $M^\wedge$ of M, then $\mathrm{H}^0(G,M)^\wedge \cong \mathrm{H}^{-1}(G, M^\wedge)$. Since $(\mathrm{H}^0(G,M)^A)^\perp = I_A \mathrm{H}^{-1}(G, M^\wedge)$, we have

$$(\mathrm{H}^0(G,M)^A)^\wedge \cong \mathrm{H}^{-1}(G, M^\wedge)/I_A\mathrm{H}^{-1}(G, M^\wedge)$$

and

$$\begin{aligned} |(\mathrm{H}^0(G,M)^A)^\wedge| &= |\mathrm{H}^{-1}(G,M^\wedge)/I_A\mathrm{H}^{-1}(G,M^\wedge)| \\ &= |\mathrm{H}^{-1}(G,M^\wedge)^A|. \end{aligned}$$

Since $(M^G)^\perp = I_G(M^\wedge)$, we see

$$(I_A \cdot M^G)^\perp = (\alpha-1)^{-1}I_G(M^\wedge),$$
$$({\mathrm{Tr}_G}^{-1}(I_A \cdot M^G))^\perp = \mathrm{Tr}_G((\alpha-1)^{-1}I_G(M^\wedge)).$$

(Here α is a generator of the cyclic group A as before.) Combining this with $(I_{G\times A}M)^\perp = (M^\wedge)^{G\times A}$, we have

$$({\mathrm{Tr}_G}^{-1}(I_A \cdot M^G)/I_{G\times A}M)^\wedge \cong (M^\wedge)^{G\times A}/\mathrm{Tr}_G((\alpha-1)^{-1}I_G(M^\wedge)).$$

Thus Proposition 3 for $M^\wedge$ implies Proposition 4 for M. □

Proposition 5 (annihilation version). *Let G be a finite abelian group and A be a finite cyclic group. Let M be a finitely generated $\mathbb{Z}[G\times A]$-module such that $M\otimes_{\mathbb{Z}}\mathbb{Q} \cong \overset{m}{\oplus}\mathbb{Q}[G\times A]$, and suppose that M is $\mathbb{Z}$-torsion free. Then we have*

$$|\mathrm{H}^0(G,M)^A| \cdot {\mathrm{Tr}_G}^{-1}(I_A \cdot M^G) \subset I_{G\times A}M.$$

Proof. By assumption M contains a $\mathbb{Z}[G\times A]$-submodule of finite index which is isomorphic to $\overset{m}{\oplus}\mathbb{Z}[G\times A]$. Put $N = M/\overset{m}{\oplus}\mathbb{Z}[G\times A]$. Then

$$\mathrm{H}^0(G,M) \cong \mathrm{H}^0(G,N)$$

as $\mathbb{Z}[A]$-modules and

$$\mathrm{H}^0(G,M)^A \cong \mathrm{H}^0(G,N)^A.$$

Moreover, we have

$$\mathrm{H}^{-1}(G\times A,M) \cong \mathrm{H}^{-1}(G\times A,N).$$

The exact sequence

$$0 \to \overset{m}{\oplus}\mathbb{Z}[G\times A] \to M \to N \to 0$$

induces the exact sequence

$$0 \to \overset{m}{\oplus}\mathbb{Z}[A] \to M^G \to N^G \to 0.$$

Therefore we have

$$\mathrm{H}^0(A, M^G) \cong \mathrm{H}^0(A, N^G).$$

It is easy to see that

$$\begin{aligned}&{\mathrm{Tr}_G}^{-1}(I_A \cdot M^G)/I_{G\times A}M \\ &\qquad\qquad \cong \mathrm{Ker}\,(\mathrm{Tr}_G : \mathrm{H}^{-1}(G \times A, M) \to \mathrm{H}^{-1}(A, M^G))\end{aligned}$$

and

$$\begin{aligned}&{\mathrm{Tr}_G}^{-1}(I_A \cdot N^G)/I_{G\times A}N \\ &\qquad\qquad \cong \mathrm{Ker}\,(\mathrm{Tr}_G : \mathrm{H}^{-1}(G \times A, N) \to \mathrm{H}^{-1}(A, N^G)).\end{aligned}$$

Hence we have

$${\mathrm{Tr}_G}^{-1}(I_A \cdot M^G)/I_{G\times A}M \cong {\mathrm{Tr}_G}^{-1}(I_A \cdot N^G)/I_{G\times A}N.$$

Therefore Proposition 4 for N proves Proposition 5 for M. □

§5. Proof of Proposition 1.

In this section, we convert the annihilation property into a comparison property of orders, and this will complete the proof of Theorem 4. Now we begin the proof of Proposition 1.

Proof of Proposition 1. Denote the homomorphisms given by projections by

$$p_1 : R \to (\overset{m}{\oplus}\mathbb{Q}[G \times A]) \oplus \mathbb{Q} \to \overset{m}{\oplus}\mathbb{Q}[G \times A]$$

and

$$p_2 : R \to (\overset{m}{\oplus}\mathbb{Q}[G \times A]) \oplus \mathbb{Q} \to \mathbb{Q}.$$

Put $R_0 = \mathrm{Ker}\, p_2$ and $R_1 = p_1(R)$. Then the short exact sequence

$$0 \to \mathrm{Ker}\, p_1 \to R \to R_1 \to 0$$

gives us the long exact sequence

$$\begin{aligned}\cdots \quad \to \quad & \mathrm{H}^{-1}(G, R) \to \mathrm{H}^{-1}(G, R_1) \to \mathrm{H}^0(G, \mathrm{Ker}\, p_1) \\ \to \quad & \mathrm{H}^0(G, R) \to \mathrm{H}^0(G, R_1) \to \mathrm{H}^1(G, \mathrm{Ker}\, p_1) \to \cdots .\end{aligned}$$

Since $\operatorname{Ker} p_1 \cong \mathbb{Z}$, we have $\mathrm{H}^0(G, \operatorname{Ker} p_1) \cong \mathbb{Z}/|G|\mathbb{Z}$ and $\mathrm{H}^1(G, \operatorname{Ker} p_1) = 0$. Thus we obtain an exact sequence

$$\begin{aligned} 0 \quad \to \quad & \operatorname{Cok}(\mathrm{H}^{-1}(G,R) \to \mathrm{H}^{-1}(G,R_1)) \to \mathbb{Z}/|G|\mathbb{Z} \\ \to \quad & \mathrm{H}^0(G,R)^A \to \operatorname{Im}(\mathrm{H}^0(G,R)^A \to \mathrm{H}^0(G,R_1)) \to 0. \end{aligned}$$

In the short exact sequence

$$0 \to R_0 \to R \to p_2(R) \to 0,$$

$p_2(R)$ is isomorphic to $\mathbb{Z}$. Therefore we have

$$\mathrm{H}^{-1}(G,R) = {\mathrm{Tr}_G}^{-1}(0)/I_G R = R_0 \cap {\mathrm{Tr}_G}^{-1}(0) \;/\; R_0 \cap I_G R.$$

Moreover, since $p_1|_{R_0} : R_0 \hookrightarrow R_1$ is injective, we see that

$$p_1(R_0 \cap {\mathrm{Tr}_G}^{-1}(0)) = p_1(R_0) \cap {\mathrm{Tr}_G}^{-1}(0).$$

Since $I_G R_1 = p_1(I_G R) \subset p_1(R_0)$, we have

$$\begin{aligned} & \operatorname{Cok}(\mathrm{H}^{-1}(G,R) \to \mathrm{H}^{-1}(G,R_1)) \\ = \quad & R_1 \cap {\mathrm{Tr}_G}^{-1}(0) \;/\; p_1(R_0) \cap {\mathrm{Tr}_G}^{-1}(0) \\ \cong \quad & R_1 \cap {\mathrm{Tr}_G}^{-1}(0) + p_1(R_0) \;/\; p_1(R_0). \end{aligned}$$

Since $I_A R \subset R_0$ and $R/R_0 \cong \mathbb{Z}$, we have

$$\mathrm{Tr}_G R \cap I_A R \subset \mathrm{Tr}_G R_0,$$

Hence we obtain

$$R^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G R = R^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G R_0,$$

where α is a generator of the cyclic group A. Note that, for $r \in R$ and $g \in G$, $(g-1)r = 0$ is equivalent to $(g-1)p_1(r) = 0$. Since $p_1|_{R_0}$ is injective, $(\alpha-1)r \in \mathrm{Tr}_G R_0$ is equivalent to $(\alpha-1)p_1(r) \in \mathrm{Tr}_G p_1(R_0)$ for $r \in R$. Hence we have

$$p_1(R^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G R_0) = R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G p_1(R_0)$$

and

$$\begin{aligned} & \operatorname{Im}(\mathrm{H}^0(G,R)^A \to \mathrm{H}^0(G,R_1)) \\ = \quad & R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G p_1(R_0) \;/\; \mathrm{Tr}_G R_1. \end{aligned}$$

Since

$$\begin{aligned}
& R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G R_1 \;/\; R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G p_1(R_0) \\
\overset{\alpha-1}{\cong}\; & I_A \cdot R_1^G \cap \mathrm{Tr}_G R_1 \;/\; I_A \cdot R_1^G \cap \mathrm{Tr}_G p_1(R_0) \\
\cong\; & (I_A \cdot R_1^G \cap \mathrm{Tr}_G R_1) + \mathrm{Tr}_G p_1(R_0) \;/\; \mathrm{Tr}_G p_1(R_0) \\
=\; & p_1(R_0) + {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G) \cap R_1 \;/\; p_1(R_0) + {\mathrm{Tr}_G}^{-1}(0) \cap R_1,
\end{aligned}$$

we have

$$\begin{aligned}
& |\mathrm{H}^0(G,R)^A|/|G| \\
=\; & |R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G p_1(R_0)/\mathrm{Tr}_G R_1| \\
& \quad / \; |R_1 \cap {\mathrm{Tr}_G}^{-1}(0) + p_1(R_0)/p_1(R_0)| \\
=\; & |R_1^G \cap (\alpha-1)^{-1}\mathrm{Tr}_G R_1/\mathrm{Tr}_G R_1| \\
& \quad / \; |p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)| \\
=\; & |\mathrm{H}^0(G,R_1)^A| \;/\; |p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)|.
\end{aligned}$$

Since $R_1/p_1(R_0) \cong \mathbb{Z}/r\mathbb{Z}$ for some $r \in \mathbb{Z}$, the subquotient

$$p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)$$

is a cyclic quotient of $R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/I_{G\times A}R_1$. Since $R_1 \otimes_{\mathbb{Z}} \mathbb{Q} \cong \overset{m}{\oplus}\mathbb{Q}[G \times A]$, Proposition 5 shows that

$$|\mathrm{H}^0(G,R_1)^A| \cdot (p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)) = 0.$$

Since $p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)$ is a cyclic group, this annihilation means that the order $|p_1(R_0) + R_1 \cap {\mathrm{Tr}_G}^{-1}(I_A \cdot R_1^G)/p_1(R_0)|$ divides $|\mathrm{H}^0(G,R_1)^A|$. Thus we have shown that $|G|$ divides $|\mathrm{H}^0(G,R)^A|$.

Therefore the proof of Proposition 1 is completely done, and hence Theorem 4 is proved now. □

References

[1] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziprozitäts-gesetz*, Abh. Math. Sem. Univ. Hamburg, **7** (1930), 46–51; Collected Papers, 159–164.

[2] Ph. Furtwängler, *Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg, **7** (1930), 14–36.

[3] D. Hilbert, *Bericht: Die Theorie der algebraischen Zahlkörper*, Jber. dt. Math.-Ver., **4** (1897), 175–546; Gesam. Abh. I., 63–363.

[4] R. C. Lyndon, *Cohomology theory of groups with a single defining relation*, Ann. of Math. (2)**52** (1950), 650–665.

[5] K. Miyake, *On the structure of the idele groups of algebraic number fields II*, Tôhoku Math. J., **34** (1982), 101–112.

[6] K. Miyake, *Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem and capitulation problem*, Expo. Math., **7** (1989), 289–346.

[7] H. Suzuki, *A generalization of Hilbert's Theorem 94*, Nagoya Math. J., **121** (1991), 161–169.

[8] F. Terada, *On a generalization of the principal ideal theorem*, Tôhoku Math. J., **1** (1949), 229–269.

Department of Mathematics, School of Science,
Nagoya University Chikusa-ku, Nagoya 464-01 Japan