On the number of crossed homomorphisms
— reduction to $p$-subgroups
(斜準同型の個数に関する予想の $p$-群への帰着)

近畿大学・理工学部　満谷 恒信 (Tsunenobu Asai)
Department of Mathematics, Kinki University

愛媛大学・理学部　庭崎 隆 (Takashi Niwasaki)
Department of Mathematics, Ehime University

This is a joint work of Yugen Takegahara, Naoki Chigira and authors.

1 Situation

Let $C$ and $H$ be groups, and suppose that $C$ acts on $H$ by a homomorphism $\varphi: C \to \text{Aut}(H)$. We indicate by $\varphi(c)(h)$ for $c \in C$ and $h \in H$. Let $H \rtimes C$ denote the semidirect product of $H$ and $C$ with canonical epimorphism $\pi: H \rtimes C \to C$.

Given a map $\lambda: C \to H$, we define a new map

$$\tilde{\lambda}: C \to H \rtimes C \quad \text{by} \quad \tilde{\lambda}(c) = \lambda(c)c.$$

Then the composition $\pi \circ \tilde{\lambda}$ coincides with the identity map $\text{id}_C$ on $C$, and conversely, a map $f: C \to H \rtimes C$ satisfying $\pi \circ f = \text{id}_C$ has the form $\tilde{\lambda}$ for some $\lambda: C \to H$. This property always underlies our arguments below. For example, we can show that

$$\lambda = \eta \iff \tilde{\lambda} = \tilde{\eta} \iff \tilde{\lambda}(C) = \tilde{\eta}(C)$$

for any maps $\lambda, \eta: C \to H$, namely, we can identify a map $\lambda$ with a suitable subset of $H \rtimes C$. Further, as subgroups of $H \rtimes C$, the normalizer $N_H(\tilde{\lambda}(D))$ coincides with the centralizer $C_H(\tilde{\lambda}(D))$ for any subset $D$ of $C$.

A map $\lambda: C \to H$ is called a crossed homomorphism (or derivation, cocycle) if $\tilde{\lambda}: C \to H \rtimes C$ is a group homomorphism, or equivalently,

$$\lambda(cd) = \lambda(c) \cdot \varphi(c)(d) \quad \text{for all} \, c, d \in C.$$

The zero-map which sends every element of $C$ to the identity element of $H$ is a crossed homomorphism. We denote by $Z^1(C, H)$ the set of crossed homomorphisms from $C$ to $H$. The most important example of $Z^1(C, H)$ is $\text{Hom}(C, H)$, the set of homomorphisms, for the trivial action of $C$ on $H$. Another well-known example is the first cocycle group of a $C$-module $H$ with respect to the bar resolution of $C$. In general, $Z^1(C, H)$ does not have a group structure unless $H$ is abelian.

For each $\lambda \in Z^1(C, H)$, we can easily verify that $\tilde{\lambda}: C \to H \rtimes C$ is a splitting monomorphism of $\pi$ (i.e., $\tilde{\lambda}$ is a homomorphism satisfying $\pi \circ \tilde{\lambda} = \text{id}_C$), and $\tilde{\lambda}(C)$ is a complements of $H$ in $H \rtimes C$ (i.e., $\tilde{\lambda}(C)$ is a subgroup of $H \rtimes C$ such that $H \cap \tilde{\lambda}(C) = 1$ and $H\tilde{\lambda}(C) = H \rtimes C$). A converse statement also holds, namely, $Z^1(C, H)$ is in one-to-one correspondence with the set of complements of $H$ in $H \rtimes C$. All of our arguments in this report can be stated in terms of complements in semidirect groups.
2 Conjecture

Only in this section, we assume that both $C$ and $H$ are finite groups. Then $Z^1(C,H)$ is finite set; we denote by $|Z^1(C,H)|$ its cardinality. A well-known theorem of Frobenius states that

$$|\{h \in H \mid h^n = 1\}| \equiv 0 \pmod{\gcd(n,|H|)}$$

for any integer $n$, which can be expressed with our notation as

$$|\text{Hom}(C,H)| \equiv 0 \pmod{\gcd(|C|,|H|)}$$

for any cyclic group $C$.

A number of proofs can be found, for example, in Brauer [5], Burnside [6], Curtis–Reiner [7], M. Hall [8], Isaacs–Robinson [10], and Zassenhaus [12]. P. Hall [9] extended the theorem to crossed homomorphisms as

$$|Z^1(C,H)| \equiv 0 \pmod{\gcd(|C|,|H|)}$$

for any cyclic group $C$.

Later, Yoshida [11] showed another generalization:

$$|\text{Hom}(C,H)| \equiv 0 \pmod{\gcd(|C|,|H|)}$$

for any abelian group $C$.

Furthermore, Yoshida and the first author of this report conjectured the following in [4].

Conjecture. Let $C'$ be the commutator subgroup of a finite group $C$. Then

$$|Z^1(C,H)| \equiv 0 \pmod{\gcd(|C/C'|,|H|)}.$$

This conjecture is still unsolved. The main theorem of this report is

Theorem 1. To prove the conjecture, we may assume that $C$ is an abelian $p$-group and $H$ is a $p$-group for a common prime $p$.

The methods and tools for the proof of Theorem 1 are the subject matter of the remaining sections. Applying our method to the argument of [4], we can also prove the following weaker result.

Theorem 2. Let $\Phi(C/C')$ denote the Frattini subgroup of $C/C'$. Then

$$|Z^1(C,H)| \equiv 0 \pmod{\gcd(|C/C'|,|H|)}.$$

On the other hand, the conjecture has been verified in the following cases ([4], [2], [3], [1]):

1. both $C$ and $H$ are abelian $p$-groups;
2. $C = \langle c \rangle \times E$, the direct product of a cyclic $p$-group $\langle c \rangle$ and an elementary abelian $p$-group $E$;
3. $C = \langle c \rangle \times \langle c_p \rangle$, where $p > 2$ and $\langle c \rangle$ is a cyclic $p$-group, while $\langle c_p \rangle$ is a cyclic group of order $p^2$;
4. $C = \langle c_1 \rangle \times \langle c_2 \rangle$, an arbitrary abelian group of rank 2, while $H$ is one of the dihedral, the semidihedral and the generalized quaternion 2-groups.

3 Group Actions

As stated in §1, the set $Z^1(C,H)$ may not have a group structure. To prove the conjecture, we need several group actions on $Z^1(C,H)$. Here we introduce the following concepts without finiteness assumption of $C$ and $H$. 


Action of $H$. For given $h \in H$ and $\lambda \in Z^1(C, H)$, the composition map

$$\text{Inn } \lambda \circ \lambda : C \longrightarrow H \times C \xrightarrow{\text{Inn } h} H \times C$$

is a splitting monomorphism of the canonical epimorphism $\pi: H \times C \to C$, where $\text{Inn } h$ is the inner automorphism by $h$. Thus the $H$-part, denoted by $^h \lambda$, of $\text{Inn } h \circ \lambda$ becomes a crossed homomorphism. More precisely, we can define $^h \lambda \in Z^1(C, H)$ by

$$(^h \lambda)(c) = (h \cdot \lambda(c) \cdot h^{-1})c^{-1} = h \cdot \lambda(c) \cdot \tilde{\lambda}(c)$$

for each $c \in C$.

In terms of complements, the well-definedness of $^h \lambda$ corresponds to the fact that the conjugate of a complement $\tilde{\lambda}(C) \leq H \times C$ by $h$ is still a complement. Therefore, $H$ acts on $Z^1(C, H)$ in this way. Note that we can show that the stabilizer of $\lambda$ in $H$ coincides with $C_H(\tilde{\lambda}(C)) = N_H(\tilde{\lambda}(C))$ as noticed in §1.

Change of Actions. Fix an element $\lambda \in Z^1(C, H)$. Then the complement $\tilde{\lambda}(C)$ acts on $H$ by conjugation in $H \times C$. This induces another action of $C$ on $H$, i.e., $C \xrightarrow{\tilde{\lambda}} H \times C \xrightarrow{\text{Inn } h} \text{Aut}(H)$. We denote by $Z^1_\lambda(C, H)$ the set of crossed homomorphisms for this action. It is easy to show that there exists a bijection

$$\lambda_\tau: Z^1_\lambda(C, H) \to Z^1(C, H)$$

given by $$(\lambda_\tau \cdot \eta)(c) = \eta(c) \lambda(c)$$

for $\eta \in Z^1_\lambda(C, H), c \in C$.

In terms of complements, this means the trivial fact that the both sets, $Z^1(C, H)$ and $Z^1_\lambda(C, H)$, correspond to the complements of $H$ in $H \times C = H \times \tilde{\lambda}(C)$. Note that this bijection induces a semi-regular action (i.e., every non-identity element has no fixed point) of the first cocycle group $Z^1(C, Z(H))$ on the set $Z^1(C, H)$, where the $C$-module $Z(H)$ denotes the center of $H$.

4 As Functors

We shall consider 'left-exactness' of $Z^1(-, -)$, although the values are objects in the category of sets where exactness is not defined.

First variable. Suppose that $D$ is a normal subgroup of $C$, namely, there exists a short exact sequence $1 \to D \to C \to C/D \to 1$ of groups. We wish to consider a problem whether there exists an exact sequence such as

$$1 \to Z^1(C/D, H_T) \to Z^1(C, H) \xrightarrow{\text{res}} Z^1(D, H),$$

where res is the restriction map and $H_T$ is some subgroup of $H$ on which $D$ acts trivially. Whereas we can not find such a common subgroup $H_T$, we can prove the following.

Theorem 3. Suppose that $\mu \in Z^1(D, H)$ is an element of $\text{res}(Z^1(C, H))$, namely, there exists an element $\lambda \in Z^1(C, H)$ such that $\text{res}(\lambda) = \mu$. Then the bijection $\lambda_\tau: Z^1_\lambda(C, H) \to Z^1(C, H)$ introduced in the previous section induces a bijection

$$\lambda_\tau: Z^1_\lambda(C/D, C_H(\tilde{\mu}(D))) \to \text{res}^{-1}(\mu).$$

For a moment, we return to the conjecture. Assume that $C$ and $H$ are finite groups, and that $D$ is a normal subgroup of $C$. Then $Z^1(C, H) = \cup_{\mu \in Z^1(D, H)} \text{res}^{-1}(\mu)$. Note that the restriction map is an $H$-map, and that the stabilizer of $\mu \in Z^1(D, H)$ in $H$ is $C_H(\tilde{\mu}(D))$. Hence it follows from Theorem 3 that

$$\left| \bigcup_{h \in H} \text{res}^{-1}(^h \mu) \right| = |H/C_H(\tilde{\mu}(D))| \cdot |\text{res}^{-1}(\mu)| = |H/C_H(\tilde{\mu}(D))| \cdot |Z^1_\lambda(C/D, C_H(\tilde{\mu}(D)))|.$$
which is divisible by $\gcd([C/D], [H])$ if $C/D$ is abelian and if the conjecture holds for $Z^1_{\lambda}(C/D, C_H(\bar{\mu}(D)))$.

This is the reason why we may assume that $C$ is an abelian $p$-group in the conjecture.

Second variable. Suppose that $K$ is a subgroup of $H$, which need not be normal nor closed under the action of $C$. Let $\text{Map}(C, K \backslash H)$ denote the set of maps from $C$ to the right cosets $K \backslash H$. We wish to consider a problem whether there exists an exact sequence such as

$$1 \to Z^1(C, K) \to Z^1(C, H) \to \text{Map}(C, K \backslash H)$$

for some subgroup $K$ of $K$; namely, we wish to describe the condition that two elements of $Z^1(C, H)$ have the same values in $K \backslash H$. For this problem, Brauer [5] gave an answer in the case where $C$ is cyclic with trivial action on $H$, i.e., $Z^1(C, H) = \text{Hom}(C, H)$. We can generalize his answer as follows.

We say that two elements $\eta, \lambda$ of $Z^1(C, H)$ are equivalent with regard to $K$, if

$$K\eta(c) = K\lambda(c) \quad \text{for all } c \in C.$$

In this case, we write $\eta \sim_K \lambda$. On the other hand, let $K_{\lambda(C)}$ denote the maximal $\lambda(C)$-invariant subgroup of $K$:

$$K_{\lambda(C)} = \bigcap_{c \in C}^{\lambda(c)} K.$$

**Proposition 4.** Let $K$ be a subgroup of $H$, and $\eta, \lambda \in Z^1(C, H)$. Then $\eta \sim_K \lambda$ if and only if $\eta \sim_{K_{\lambda(C)}} \lambda$.

In other words, if $\eta \sim_K \lambda$, then $\eta(c)\lambda(c)^{-1} \in K_{\lambda(C)}$.

**Theorem 5.** Let $K$ be a subgroup of $H$, and $\lambda \in Z^1(C, H)$. Then the bijection $\lambda_r: Z^1_{\lambda}(C, H) \to Z^1(C, H)$ induces the bijection

$$\lambda_r: Z^1_{\lambda}(C, K_{\lambda(C)}) \to \{ \eta \in Z^1(C, H) \mid \eta \sim_K \lambda \}.$$  

This is an answer of the problem above, whereas a common subgroup $K$ can not be taken. Further, Brauer [5] introduced another equivalence relation, which can be generalized as follows.

We say that two elements $\eta, \lambda$ of $Z^1(C, H)$ are weakly equivalent with regard to $K$, if there exists an element $k \in K$ such that $\eta \sim_K k\lambda$, where $k\lambda$ is defined in the previous section. In this case, we write $\eta \approx_K \lambda$.

**Theorem 6.** Let $K$ be a subgroup of $H$, $k \in K$ and $\lambda \in Z^1(C, H)$. Then $\lambda \sim_K k\lambda$ if and only if $k \in K_{\lambda(C)}$. Therefore we have a bijection

$$\{ \eta \in Z^1(C, H) \mid \eta \approx_K \lambda \} = \bigcup_{k \in [K/K_{\lambda(C)}]} \{ \eta \in Z^1(C, H) \mid \eta \sim_K k\lambda \}$$

$$\simeq \bigcup_{k \in [K/K_{\lambda(C)}]} Z^1_{\lambda}(C, K_{\lambda(C)}),$$

where $[K/K_{\lambda(C)}]$ denotes a complete set of representatives of $K/K_{\lambda(C)}$.

We return to the conjecture. Assume that $C$ and $H$ are finite groups, and that $K$ is a subgroup of $H$. Then $Z^1(C, H)$ is the union of the weakly equivalence classes with regard to $K$. However, it follows from Theorem 6 that

$$|\{ \eta \in Z^1(C, H) \mid \eta \approx_K \lambda \}| = |K/K_{\lambda(C)}| \cdot |Z^1_{\lambda}(C, K_{\lambda(C)})|.$$
which is divisible by \( \gcd(|C/C'|, |K|) \) if the conjecture holds for \( Z^1_\tilde{\lambda}(C, K_{\tilde{\lambda}(C)}) \). This is the reason why we may assume that \( H \) is a \( p \)-group in the conjecture.

Finally, we remark that if \( K \) is closed under the action of \( \tilde{\lambda}(C) \), then \( \sim_K \) and \( \approx_K \) are the same relation. In [1], we used \( \sim_K \) to calculate \( |Z^1(C, H)| \), where \( H \) is an exceptional 2-group and \( K \) is a characteristic subgroup of \( H \).

References


