数理解析研究所講究録
第 877 巻 1994 年 1-5

On congruences concerning the number of group homomorphisms between groups

Tsunenobu Asai
Department of Mathematics, Kinki University

This work is a joint work with T.Yoshida and Y.Takegahara. The almost results in this report are found in [AY].

Let A and G be finite groups. We consider the congruences concerning the number of group homomorphisms from A to G, $|\mathrm{Hom}(A,G)|$. For a subgroup B of A and any homomorphism μ from B to G, we denote by $H(A,G;B,\mu)$ the set of group homomorphisms from A to G whose restriction to B is μ, i.e. $H(A,G;B,\mu) := \{\lambda \in \mathrm{Hom}(A,G) \mid \lambda_{|B} = \mu\}$. In [Yo2], Yoshida proved the following theorem.

Theorem [Yo2]: *Let G be a finite group, A a finite abelian group and B a subgroup of A. Then for any homomorphism μ from B to G,*

$$|H(A,G;B,\mu)| \equiv 0 \qquad \mathrm{mod}\ \gcd\left(|A/B|, |C_G(\mu(B))|\right).$$

Especially,

$$|\mathrm{Hom}(A,G)| \equiv 0 \quad \mathrm{mod}\ \gcd(|A|,|G|).$$

Here we want to generalize the above theorem, and we consider the following two conjectures.

Conjecture I: *Let G and A be finite groups and B a subgroup of A. Then for any homomorphism μ from B to G,*

$$(\mathrm{CI}): \qquad |H(A,G;B,\mu)| \equiv 0 \qquad \mathrm{mod}\ \gcd\left(|A/A'B|, |C_G(\mu(B))|\right),$$

where A' is the commutator subgroup of A. Especially,

$$|\mathrm{Hom}(A,G)| \equiv 0 \quad \mathrm{mod}\ \gcd(|A/A'|,|G|).$$

Conjecture I seems to be quite natural. In fact, that is true in some special cases, but we can not prove yet in general. Later, we give some weaker congruences in general situation as Theorem 2.

Conjecture II is another type congruence which is concerned with the number of cocycles. Let C and H be finite groups such that C acts on H, and denote by ${}^{c}h$ this action of $c \in C$ on $h \in H$. We denote $Z^1(C,H)$ for the set of cocycles i.e.

$$Z^1(C,H) := \{\eta : C \longrightarrow H \mid \eta(cc') = \eta(c) \cdot {}^{c}\eta(c') \quad \text{for } c, c' \in C\}.$$

Let $X := HC \trianglerighteq H$ be the semidirect product of H by C. Then it is easily proved that $|Z^1(C,H)|$ is equal to the number of complements for H in X i.e.

$$|Z^1(C,H)| = \sharp\{D \leq X \mid X = HD, H \cap D = 1\}.$$

Conjecture II: *Let C be an abelian p-group and H a nilpotent group such that C acts on H. Then*

$$\text{(CII)}: \qquad |Z^1(C,H)| \equiv 0 \mod \gcd(|C|, |H|).$$

Relation Conjecture I and II

Conjecture I and II are closely related, the following theorem shows the relation.

Theorem 1: *If* (CII) *is true, then so is* (CI).

We briefly sketch the proof of Theorem 1.

(Sketch of the proof): Let $(A, G; B, \mu)$ be a counter example to (CI) such that

$(A : B)$ is minimal;
Under the above, $|G|$ is minimal;
Under the above, $|A|$ is minimal.

Step 1: We may consider under the following situation:

$B \trianglelefteq A$ and A/B is an abelian p-group.
$\mu : B \longrightarrow G$ is a monomorphism.
$\mu(B) \trianglelefteq G$ and $G/\mu(B)$ is a p-group.
$H := C_G(\mu(B)) \trianglelefteq G$ and H is a nilpotent group.

Under these conditions, we next define an equivalence relation $\approx_H$ on $H(A, G; B, \mu)$. For $\lambda, \lambda' \in H(A, G; B, \mu)$,

$$\lambda \approx_H \lambda' \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \lambda'(a) \in H\lambda(a) \quad \text{for all } a \in A.$$

For any $\lambda_0 \in H(A, G; B, \mu)$, we set

$$[\lambda_0] := \{\lambda \in H(A, G; B, \mu) \mid \lambda \approx_H \lambda_0\}.$$

If $\sharp[\lambda_0] \equiv 0 \mod \gcd(|A/B|, |H|_p)$ is true, then so is (CI).

Step 2: Take any $\lambda_0 \in H(A, G; B, \mu)$. Then A/B acts on H by

$$^{aB}h := \lambda_0(a) h \lambda_0(a)^{-1}$$

for $a \in A$, $h \in H$. There is a one to one correspondence between

$$[\lambda_0] \Longleftrightarrow Z^1(A/B, H).$$

Step 2 shows that if (CII) is true, then so is (CI).

By Theorem 1, we consider when Conjecture II holds.

Proposition 1: *If C is an elementary abelian p-group, then* Conjecture II *is true.*

PROOF: We may assume that H is a nontrivial p-group. Let $X := HC$, and $Z := \Omega_1(Z(X) \cap H)$. Here note that $Z \neq 1$, because X is a p-group and H is a normal subgroup of X. Now $\mathrm{Hom}(C, Z)$ acts on $Z^1(C, H)$ by multiplication, i.e.

$$\begin{array}{ccc} \mathrm{Hom}(C, Z) \times Z^1(C, H) & \longrightarrow & Z^1(C, H) \\ (f, \eta) & \longmapsto & (f\eta : c \mapsto f(c) \cdot \eta(c)). \end{array}$$

Since this action is semi-regular, that is, any nontrivial element of $\mathrm{Hom}(C, Z)$ has no fixed points, we have

$$|Z^1(C, H)| \equiv 0 \qquad \mod |\mathrm{Hom}(C, Z)|.$$

Since C is elementary abelian and $Z \neq 1$,

$$|\mathrm{Hom}(C, Z)| \equiv 0 \qquad \mod |C|,$$

and hence

$$|Z^1(C, H)| \equiv 0 \qquad \mod |C|.$$

Proposition 2: *If C is a cyclic p-group, then* Conjecture II *is true.*

PROOF: We may assume that H is a nontrivial p-group. Let $X := HC$. First we construct a central series of subgroups of H,

$$1 = Z_0 \leq Z_1 \leq Z_2 \leq \cdots \leq H,$$

$$\begin{aligned} Z_1 &:= \Omega_1(Z(X) \cap H), \\ Z_i/Z_{i-1} &:= \Omega_1(Z(X/Z_{i-1}) \cap H/Z_{i-1}). \end{aligned}$$

Then $\{Z_i\}$ has the following properties:

Z_i is a normal subgroup of X.
If Z_i is a proper subgroup of H, then $Z_{i+1}/Z_i \neq 1$ and $|Z_i| \geq p^i$.
For any $z \in Z_i$, $z^p \in Z_{i-1}$ and $z^{p^i} = 1$.
For any $z \in Z_i$ and any $x \in X$, $x^{p^i} = (zx)^{p^i}$.

Let $C = \langle c \rangle$ and $|C| = p^n$. Then Z_n acts on the set of complements for H in X by multiplication, i.e.

$$\begin{array}{ccc} Z_n \times \mathcal{C} & \longrightarrow & \mathcal{C} \\ (z, \langle hc \rangle) & \longmapsto & \langle zhc \rangle, \end{array}$$

where $\mathcal{C} := \{\langle hc \rangle \leq X \mid h \in H, X = H\langle hc \rangle, H \cap \langle hc \rangle = 1\}$ is the set of complements for H in X. This action is semi-regular and $|\mathcal{C}| = |Z^1(C,H)|$. So we have that if $Z_n = H$, then

$$|Z^1(C,H)| \equiv 0 \qquad \mathrm{mod}\ |H|,$$

and if Z_n is a proper subgroup of H, then $|Z_n| \geq p^n = |C|$, and so

$$|Z^1(C,H)| \equiv 0 \qquad \mathrm{mod}\ |C|.$$

Hence in either case, we have

$$|Z^1(C,H)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|C|, |H|).$$

By Theorem 1 and Proposition 2 and 3, we have the following theorems.

Theorem 2: *Let A, G be finite groups and B a subgroup of A. For any homomorphism μ from B to G,*

$$|H(A,G;B,\mu)| \equiv 0 \quad \mathrm{mod}\ \gcd\left(((A/A'B) : \Phi(A/A'B)), |C_G(\mu(B))|\right),$$

where A' is the commutator subgroup of A and $\Phi(A/A')$ is the Frattini subgroup of A/A'. Especially,

$$|\mathrm{Hom}(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd\left(((A/A') : \Phi(A/A')), |G|\right).$$

Theorem 3: *Let A, G be finite groups such that A/A' is cyclic. Then for any subgroup B of A and any homomorphism μ from B to G,*

$$|H(A,G;B,\mu)| \equiv 0 \qquad \mathrm{mod}\ \gcd\left((A/A'B), |C_G(\mu(B))|\right).$$

Especially,

$$|\mathrm{Hom}(A,G)| \equiv 0 \qquad \mathrm{mod}\ \gcd(|A/A'|, |G|).$$

In Hall [Ha], we can find the essentially same theorem as Theorem 3.

Concerning Conjecture II

Conjecture II is not proved yet in general. But in several special cases, Conjecture II holds. For example, if H is an abelian, then Conjecture II is true. In this case, we can prove that by using Hochschild and Serre exact sequence of cohomology [Su, (7.29)] and the induction of the rank of C.

References

[AY] T. Asai and T. Yoshida, $|\mathrm{Hom}(A,G)|$, II, *Journal of Algebra*, **160**(1) (1993), 273–285.

[Ha] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1935), 468–501.

[Su] M. Suzuki, Group Theory I, Springer–Verlag, Berlin–Heidelberg–New York, 1982.

[Yo2] T. Yoshida, $|\mathrm{Hom}(A,G)|$, *J. Algebra*, **156** (1993), 125–156.