

$|\mathbf{Hom}(A, G)|$ (III)

Tomoyuki Yoshida

§1. Introduction

For a finite group G , its *Frobenius number* h_n^{cyc} is the number of solutions of the equation $x^n = 1$ in G and a *Sylow number* s_n^{cyc} is the number of cyclic subgroups of G of order n . These numbers are named after Frobenius theorem and Sylow's theorem ([Yo 96]). The classical Frobenius theorem states that h_n^{cyc} is divisible by the greatest common divisor of n and $|G|$. The following *transition formula* holds:

$$(1) \quad h_n^{\text{cyc}} = \sum_{r|n} \varphi(r) s_r^{\text{cyc}}, \quad (n \geq 1),$$

where φ denotes the Euler function.

Now define the *zeta functions of Sylow and Frobenius types* by

$$S_G^{\text{cyc}}(z) := \sum_{n=1}^{\infty} \frac{\varphi(n) s_n^{\text{cyc}}}{n^z} = \sum_{g \in G} |g|^{-z},$$
$$H_G^{\text{cyc}}(z) := \sum_{n=1}^{\infty} \frac{h_n^{\text{cyc}}}{n^z}.$$

Then the transition formula can be presented by the *transition identity* between these functions as follows:

$$(2) \quad H_G^{\text{cyc}}(z) = \zeta(z) S_G^{\text{cyc}}(z),$$

where the transition function $\zeta(z)$ is Riemann's zeta function. Another expression of the transition formula (1) is given by the following *cyclo-tomic identity*:

$$(3) \quad \prod_{n=1}^{\infty} \left(\frac{1}{1-t^n} \right)^{\#\{g \in G \mid |g|=n\}/n} = \exp \left(\sum_{n=1}^{\infty} \frac{h_n^{\text{cyc}}}{n} t^n \right).$$

Received April 20, 1999.

Revised July 11, 2000.

Here we note that the number h_n^{cyc} equals the number of group homomorphisms from a cyclic group C_n of order n to the group G :

$$h_n^{\text{cyc}} = h(C_n, G) := |\text{Hom}(C_n, G)|.$$

The purpose of this paper is to generalize the above formulas (1), (2) to more general classes of groups

The most of notation and terminology in this paper are standard (cf. [Su 82]). The symbol $\Omega_1(A)$ for a group A denotes the subgroup generated by elements of prime order; C_n denotes a cyclic group of order n ; C_p^r denotes an elementary abelian p -group of order p^r .

§2. Frobenius numbers and Sylow numbers.

For any finite groups A and B , put

$$\begin{aligned} h(A, B) &:= |\text{Hom}(A, B)|, \\ q(A, B) &:= \#\{A_1 \trianglelefteq A \mid A/A_1 \cong B\}, \\ s(A, B) &:= \#\{A_1 \subseteq B \mid A_1 \cong A\}. \end{aligned}$$

We call $h(A, B)$ (resp. $s(A, B)$) a *Frobenius* (resp. *Sylow*) *number*. The following lemma easily follows from the homomorphism theorem:

Lemma 2.1 (Transition formula). *For any finite groups A and G ,*

$$\begin{aligned} h(A, G) &= \sum'_B \#\{A_1 \trianglelefteq A \mid A/A_1 \cong B\} \cdot |\text{Aut}B| \cdot s(B, G) \\ &= \sum_{A_1 \trianglelefteq A} |\text{Aut}(A/A_1)| \cdot s(A/A_1, G). \end{aligned}$$

where B runs over all isomorphism classes of finite groups.

Now, let μ (resp. μ_A^n) be the Möbius function of the lattice of subgroups (resp. normal subgroups) of a finite group A .

Lemma 2.2. *Assume that A is a finite nilpotent group with $B \leq C \leq A$. $A_{(p)}, B_{(p)}, C_{(p)}$ denote the Sylow p -subgroups of A, B, C , respectively.*

- (i) $\mu_A^n(B, C) = \mu_{A/B}^n(1, C/B)$.
- (ii) $\mu(B, C) = \prod_p \mu(B_{(p)}, C_{(p)})$, $\mu_A^n(1, B) = \prod_p \mu_{A_{(p)}}^n(1, B_{(p)})$.
- (iii) If $\mu_A^n(1, B) \neq 0$, then B is a subgroup of $\Omega_1(Z(A))$.
- (iv) When C is a p -group,

$$\mu(B, C) = \begin{cases} (-1)^r p^{\binom{r}{2}} & \text{if } B \trianglelefteq C \text{ and } C/B \cong C_p^r \\ 0 & \text{else.} \end{cases}$$

(v) When A is a p -group,

$$\mu_A^n(1, B) = \begin{cases} \mu(1, B) = (-1)^r p^{\binom{r}{2}} & \text{if } C_p^r \cong B \leq \Omega_1(Z(A)) \\ 0 & \text{if } B \not\leq \Omega_1(Z(A)). \end{cases}$$

PROOF. Refer to [St 97, Section 3.9, 10].

Proposition 2.3 (Inversion formula). *For any finite group A and G ,*

$$(4) \quad s(A, G) = \frac{1}{|\text{Aut}(A)|} \sum_{B \trianglelefteq A} \mu_A^n(1, B) h(A/B, G).$$

Proof. Submitting the identity (Lemma 2.1)

$$h(A/B, G) = \sum_C' q(A/B, C) |\text{Aut}(C)| s(C, G)$$

to the right hand side of (4), we have

$$\begin{aligned} \text{RHS} &= \frac{1}{|\text{Aut}(A)|} \sum_{B \trianglelefteq A} \mu_A^n(1, B) \sum_C' q(A/B, C) |\text{Aut}(C)| s(C, G) \\ &= \frac{1}{|\text{Aut}(A)|} \sum_C' \left(\sum_{B \trianglelefteq A} \mu_A^n(1, B) q(A/B, C) \right) |\text{Aut}(C)| s(C, G). \end{aligned}$$

The inner summation is equal to

$$\begin{aligned} \sum_{B \trianglelefteq A} \dots &= \sum_{B \trianglelefteq A} \mu_A^n(1, B) \cdot \#\{B_1/B \trianglelefteq A/B \mid A/B_1 \cong C\} \\ &= \sum_{\substack{B_1 \trianglelefteq A \\ :A/B_1 \cong C}} \sum_{\substack{B \trianglelefteq A \\ :B \subseteq B_1}} \mu_A^n(1, B) \\ &= \sum_{\substack{B_1 \trianglelefteq A \\ :A/B_1 \cong C}} \delta(1, B_1) = \begin{cases} 1 & \text{if } A \cong C \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Hence the right hand side of (4) is equal to $s(A, G)$.

Q.E.D.

Corollary 2.4 (Inversion formula for nilpotent groups). *For any finite nilpotent group A and for any finite group G ,*

$$(5) \quad s(A, G) = \frac{1}{|\text{Aut}(A)|} \sum_{B \leq \Omega_1(Z(A))} \mu(1, B) h(A/B, G).$$

§3. Zeta functions of Sylow type.

Let \mathcal{A} be a family of finite groups closed under isomorphisms and quotient groups. Furthermore, let $w : \mathbb{N} \rightarrow R$ be a mapping to a commutative complete topological ring R containing the rational number field \mathbb{Q} . Then the *zeta function of Sylow type* of the finite group G with respect to \mathcal{A} and w is defined by

$$S(\mathcal{A}, w, G) := \sum'_{A \in \mathcal{A}/\cong} s(A, G)w(|A|) = \sum'_{\substack{A \leq G \\ A \in \mathcal{A}}} w(|A|).$$

Note that \mathcal{A} can be replaced by the finite (up to isomorphism) family consisting of those members of \mathcal{A} which are involved in the group G .

Theorem 3.1 (Transition formula). *Assume that the family \mathcal{A} consists of some nilpotent groups. Then the following holds:*

$$(6) \quad S(\mathcal{A}, w, G) = \sum'_{C, B} \frac{\mu(1, B)w(|B| \cdot |C|)|\text{Ext}(C, B; \mathcal{A})|}{|\text{Aut}(B)| \cdot |\text{Aut}(C)| \cdot |\text{Hom}(C, B)|} h(C, G),$$

where C (resp. B) runs over a complete set of representatives of \mathcal{A}/\cong (resp. abelian groups such that $B = \Omega_1(B)$). Furthermore, $\text{Ext}(C, B; \mathcal{A})$ denotes the set of equivalence classes of central extensions:

$$\text{Ext}(C, B; \mathcal{A}) = \{1 \rightarrow B \rightarrow A(\in \mathcal{A}) \rightarrow C \rightarrow 1(\text{c.e.})\}/\cong.$$

Proof. First, by the inversion formula,

$$\begin{aligned} S(\mathcal{A}, w, G) &= \sum'_{A \in \mathcal{A}} s(A, G)w(|A|) \\ &= \sum'_{A \in \mathcal{A}} \sum_{B \leq Z(A)} \mu(1, B)h(A/B, G) \frac{w(|A|)}{|\text{Aut}(A)|} \\ &= \sum'_{A \in \mathcal{A}} \sum'_{C \in \mathcal{A}} \sum_{\substack{B \leq Z(A) \\ A/B \cong C}} \mu(1, B)h(A/B, G) \frac{w(|A|)}{|\text{Aut}(A)|} \\ &= \sum'_{A \in \mathcal{A}} \sum'_{C \in \mathcal{A}} \sum'_{\substack{B: \text{abel} \\ B \rightarrow A \rightarrow C(\text{c.e.})}} \sum \frac{\mu(1, B)h(C, G)w(|A|)}{|\text{Aut}(A)| |\text{Aut}(B)| |\text{Aut}(C)|}, \end{aligned}$$

where the most inner summation is taken over all central extensions:

$$1 \rightarrow B \rightarrow A(\in \mathcal{A}) \rightarrow C \rightarrow 1.$$

The equivalence of two such central extensions is defined by

$$(1 \rightarrow B \xrightarrow{\varphi} A \xrightarrow{\psi} C \rightarrow 1) \sim (1 \rightarrow B \xrightarrow{\varphi'} A \xrightarrow{\psi'} C \rightarrow 1) \\ \iff \exists \alpha \in \text{Aut}(A) \text{ s.t. } \alpha \circ \varphi = \varphi', \psi = \psi' \circ \alpha.$$

By extension theory of groups, the number of such central extensions equivalent to a given $B \twoheadrightarrow A \rightarrow C$ is equal to

$$\frac{|\text{Aut}(A)|}{|\text{Hom}(C, B)|}.$$

Thus

$$S(\mathcal{A}, w, G) \\ = \sum'_{A \in \mathcal{A}} \sum'_{C \in \mathcal{A}} \sum'_{B: \text{abel}} \sum_{[B \twoheadrightarrow A \rightarrow C \text{ (c.e.)}]} \frac{\mu(1, B)h(C, G)w(|A|)}{|\text{Hom}(C, B)| |\text{Aut}(B)| |\text{Aut}(C)|} \\ = \sum'_{A \in \mathcal{A}} \sum'_{C \in \mathcal{A}} \sum'_{B: \text{abel}} \sum_{[B \twoheadrightarrow A \rightarrow C \text{ (c.e.)}]} \frac{\mu(1, B)h(C, G)w(|B| \cdot |C|)}{|\text{Hom}(C, B)| |\text{Aut}(B)| |\text{Aut}(C)|} \\ = \sum'_{C, B} \frac{\mu(1, B)w(|B| \cdot |C|)|\text{Ext}(C, B; \mathcal{A})|}{|\text{Aut}(B)| |\text{Aut}(C)| |\text{Hom}(C, B)|} h(C, G).$$

Remark. For the class of finite nilpotent groups, (6) does not converge.

Applying Theorem 3.1 to the family \mathcal{C} of cyclic groups, we have the formula (1) in Introduction. In this case,

$$|\text{Ext}(C_n, C_m; \mathcal{C})| = \varphi(m)\varphi(n)\text{gcd}(m, n)/\varphi(mn).$$

Next, applying Theorem 3.1 to the family \mathcal{A}_p of abelian p -groups, we have the transition formula as follows:

$$(7) \quad \frac{H_G^{A_p}(x)}{S_G^{A_p}(x)} = \prod_{m=1}^{\infty} (1 - p^{-m}x)^{-1},$$

where

$$H_G^{A_p}(x) := \sum_{n=0}^{\infty} \sum'_{|A|=p^n} \frac{h(A, G)}{|\text{Aut}(A)|} x^n, \\ S_G^{A_p}(x) := \sum_{n \geq 0} \sum'_{|A|=p^n} s(A, G)x^n.$$

This funny identity with $G = 1, x = 1$ implies P.Hall's strange formula:

$$(8) \quad \sum_A' \frac{1}{|\text{Aut}(A)|} = \sum_A' \frac{1}{|A|},$$

where A runs over all classes of abelian p -groups ([Yo 92]).

§4. Partition identities.

Let \mathcal{E}_p be the family of all elementary abelian p -groups. As is well-known, the following hold:

$$\begin{aligned} |\text{Ext}(C_p^s, C_p^r; \mathcal{E}_p)| &= 1, \\ \#\{B \subseteq C_p^n \mid |B| = p^r\} &= \begin{bmatrix} n \\ r \end{bmatrix}_p := \frac{[p]_n}{[p]_r [p]_{n-r}}, \\ [p]_n &= (p-1)(p^2-1) \cdots (p^n-1), \\ |\text{Aut}(C_p^n)| &= |\text{GL}(n, p)| = p^{\binom{n}{2}} [p]_n, \\ \mu(1, C_p^r) &= (-1)^r p^{\binom{r}{2}}. \end{aligned}$$

Thus Lemma 2.1 and Proposition 2.3 have the following forms:

$$(9) \quad h(C_p^n, G) = \sum_{r=0}^n \begin{bmatrix} n \\ r \end{bmatrix}_p \cdot |\text{GL}(r, p)| s(C_p^r, G),$$

$$(10) \quad s(C_p^n, G) = \frac{1}{|\text{GL}(n, p)|} \sum_{r=0}^n (-1)^r p^{\binom{r}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_p h(C_p^{n-r}, G).$$

We take the weight function w of the form $w(p^n) = f(n)x^n$, so that by Theorem 3.1, we have

$$\begin{aligned} S_{G,f}^{E_p}(x) &:= \sum_{n \geq 0} s(C_p^n, G) f(n) x^n \\ &= \sum_{r,s \geq 0} \frac{(-1)^r p^{\binom{r}{2}} f(r+s) h(C_p^s, G)}{|\text{GL}(r, p)| \cdot |\text{GL}(s, p)| \cdot p^{rs}} x^{r+s} \\ (11) \quad &= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{f(r+n)}{[p]_r} (-p^{-n}x)^r \right) \frac{h(C_p^n, G)}{|\text{GL}(n, p)|} x^n. \end{aligned}$$

Case $f(n) = 1$. In this case, (11) gives

$$\begin{aligned}
 S_{G,1}^{\text{E}_p}(x) &= \sum_{n \geq 0} s(C_p^n, G) x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{1}{[p]_r} (-p^{-n}x)^r \right) \frac{h(C_p^n, G)}{|\text{GL}(n, p)|} x^n \\
 (12) \quad &= \prod_{r=1}^{\infty} (1 - p^{-r}x) \cdot \sum_{n=0}^{\infty} \left(\prod_{r=1}^n (1 - p^{-r}x)^{-1} \right) \frac{h(C_p^n, G)}{|\text{GL}(n, p)|} x^n.
 \end{aligned}$$

Here we used the q -binomial theorem:

$$(13) \quad \sum_{r=0}^{\infty} \frac{1}{[p]_r} (-p^{-n}x)^r = \prod_{r=1}^{\infty} (1 - p^{-n-r}x).$$

Even if the group G is trivial, (12) gives a non-trivial formula called Cauchy's identity (1893) and then Euler's one:

$$(14) \quad \prod_{r=1}^{\infty} (1 - p^{-r}x)^{-1} = \sum_{n=0}^{\infty} \left(\prod_{i=1}^n (1 - p^{-i}x)^{-1} \right) \frac{x^n}{|\text{GL}(n, p)|},$$

$$(15) \quad \prod_{r=1}^{\infty} (1 - p^{-r})^{-1} = \sum_{n=0}^{\infty} \left(\prod_{i=1}^n (p^i - 1)^{-2} \right) p^n.$$

Case $f(n) = p^{\binom{n}{2}}$. In this case, (11) gives

$$\begin{aligned}
 S_{G,f}^{\text{E}_p}(x) &:= \sum_{n \geq 0} s(C_p^n, G) p^{\binom{n}{2}} x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{p^{\binom{n}{2} + \binom{r}{2}}}{[p]_r} (-x)^r \right) \frac{h(C_p^n, G)}{|\text{GL}(n, p)|} x^n, \\
 &= \left(\sum_{r=0}^{\infty} \frac{p^{\binom{r}{2}}}{[p]_r} (-x)^r \right) \cdot \left(\sum_{n=0}^{\infty} \frac{h(C_p^n, G)}{[p]_n} x^n \right), \\
 (16) \quad &= \prod_{r=1}^{\infty} (1 + p^{-r}x)^{-1} \cdot \left(\sum_{n=0}^{\infty} \frac{h(C_p^n, G)}{[p]_n} x^n \right).
 \end{aligned}$$

Here we used the q -binomial theorem. Hence, we conclude that

$$(17) \quad \frac{H_{G,f}^{\text{E}_p}(x)}{S_{G,f}^{\text{E}_p}(x)} = \prod_{r=1}^{\infty} (1 + p^{-r}x),$$

where

$$H_{G,f}^{\mathbb{E}_p}(x) := \sum_{n=0}^{\infty} \frac{h(C_p^n, G)}{[p]_n} x^n. \quad (|x| < p).$$

Remark. As rational functions over the complete p -adic number field, we have

$$(18) \quad \frac{H_{G,f}^{\mathbb{E}_p}(x)}{S_{G,f}^{\mathbb{E}_p}(x)} = \prod_{r=0}^{\infty} (1 + p^r x)^{-1}.$$

A special value of $S_{G,f}^{\mathbb{E}_p}(x)$ is related with the Euler characteristic $\chi(\mathcal{S}_p(G))$ of the poset of non-trivial p -subgroups:

$$(19) \quad \chi(\mathcal{S}_p(G)) := \sum_{A, B \neq 1} \mu(A, B) = - \sum_{B \neq 1} \mu(1, B),$$

where A, B run over all nontrivial p -subgroups and μ is the Möbius function of the subgroup lattice of G . Thus Lemma 2.2(iv) implies the following:

Lemma 4.1. *Under the above notation, the following holds:*

$$(20) \quad S_{G,f}^{\mathbb{E}_p}(-1) = 1 - \chi(\mathcal{S}_p(G)).$$

For $n \geq 0$, we define the numbers χ'_n 's by

$$\chi'_n := \sum_{r=0}^n (-1)^r p^{\binom{r}{2}} s(C_p^r, G).$$

Then $1 - \chi'_n$ is equal to the Euler characteristic of the poset of p -subgroups of G of order at most p^n . By the inversion formula (10), we have

$$(21) \quad [p]_n \chi'_n = \sum_{r=0}^n (-1)^{n-r} p^{\binom{r+1}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_p h_{n-r}.$$

Consider the following generating series associated to the series $\{\chi'_n\}_{n \geq 0}$:

$$X_G(t) := \sum_{n=0}^{\infty} \chi'_n (-t)^n.$$

Then we have

$$\begin{aligned} X_G(t) &= \sum_{n=0}^{\infty} \sum_{r=0}^n (-1)^r p^{\binom{r}{2}} s(C_p^r, G) (-t)^n \\ &= (1+t)^{-1} \sum_{r=0}^{\infty} p^{\binom{r}{2}} s(C_p^r, G) t^r \\ &= (1+t)^{-1} S_{G,f}^{E_p}(t). \end{aligned}$$

Thus the transition identity (16) gives

$$(22) \quad X_G(t) = \prod_{n=0}^{\infty} (1 + p^{-n}t)^{-1} \cdot H_{G,f}^{E_p}(t).$$

Similarly, if we view $X_G(t)$ and $H_{G,f}^{E_p}(t)$ as p -adic power series (18), we have

$$(23) \quad X_G(t) = \prod_{n=1}^{\infty} (1 + p^n t) \cdot H_{G,f}^{E_p}(t).$$

These formula gives a transition formula between $\{h_n\}$ and $\{\chi'_n\}$:

$$(24) \quad h_n = \sum_{r=0}^n (-1)^r p^{n-r} \begin{bmatrix} n \\ r \end{bmatrix}_p \chi'_r.$$

By (21) and (24), if p^n divides $|G|$, then

$$(25) \quad \chi'_n \equiv 0 \pmod{p^n} \iff h_n \equiv 0 \pmod{p^n}.$$

The right hand side of this statement is valid by [Yo 93]. Thus we again have Brown's cohomological Sylow theorem ([Yo 96]):

$$(26) \quad \chi(\mathcal{S}_p(G)) \equiv 1 \pmod{|G|_p}.$$

References

- [St 97] R.P. Stanley, *Enumerative Combinatorics, Volume I*, Cambridge University Press, 1997.
- [Su 82] M. Suzuki, *Group Theory, I, II*, Springer, 1982.
- [Yo 92] T. Yoshida, P.Hall's strange formula for abelian p -groups, *Osaka Math.J.*, **29** (1992), 421-431.
- [Yo 93] T. Yoshida, |Hom(A, G)|, *J. Algebra*, **156** (1993), 125-156.

- [Yo 96] T. Yoshida, Classical problems in group theory (I): Enumerating subgroups and homomorphisms, *Sugaku Expositions*, **9** (1996), 169–184.

Department of Mathematics
Hokkaido University
Sapporo 060-0810, Japan
e-mail: yoshidat@math.sci.hokudai.ac.jp