J.Math.Univ.Tokushima
Vol.35 (2001), 1-8

Zeta Functions of Finite Groups and Arithmetically Equivalent Fields

By

Shin-ichi KATAYAMA

Faculty of Integrated Arts and Sciences
The University of Tokushima
1-1, Minamijosanjima-cho
Tokushima-shi, 770-8502, JAPAN
e-mail address: *katayama@ias.tokushima-u.ac.jp*
(Received September 14, 2001)

Abstract

Recently in [4], we have investigated several zeta functions associated to finite groups and introduced a new equivalence relation on finite groups. In this paper, we shall study some relations between this equivalence relation and the corresponding Galois groups of arithmetically equivalent fields more precisely.

2000 Mathematics Subject Classification. Primary 11M41; Secondary 11R42, 20D60

Introduction

Recently, several zeta functions associated to finite groups were introduced and investigated in [4] and [9]. Using these zeta functions, we have introduced in [4] a new equivalence relation on finite groups. We applied this new equivalence relation to the construction of arithmetically equivalent fields.

The purpose of this paper is to investigate the relations of the above equivalence relation introduced in [4] and the arithmetically equivalent fields more precisely.

We will use the following notations. Let G be a finite group. We denote the order of G by $|G|$ and the order of an element $x \in G$ by $|x|$. Let $\mathbf{Z}/n\mathbf{Z}$ be the cyclic group of order n. We define the following arithmetic functions associated to the finite group G:

$$\begin{aligned} s_G(n) &= \#\{H < G | H \cong \mathbf{Z}/n\mathbf{Z}\}, \\ O_G(n) &= \#\{x \in G | |x| = n\}, \\ h_G(n) &= \#\{x \in G | x^n = 1\}, \end{aligned}$$

where $s_G(n)$ and $h_G(n)$ are called the *Sylow number* and the *Frobenius number*. We note that the Sylow number and the Frobenius number are related to the classical theorems on finite groups of Sylow and Frobenius, respectively.

According to [4] and [9], we shall call the following generating functions of the above arithmetic functions the *zeta functions* of the finite group G:

$$\begin{aligned} \zeta(G,s) &= \sum_{n=1}^{\infty} \frac{s_G(n)}{n^s}, \\ \zeta_S(G,s) &= \sum_{n=1}^{\infty} \frac{O_G(n)}{n^s}, \\ \zeta_H(G,s) &= \sum_{n=1}^{\infty} \frac{h_G(n)}{n^s}, \end{aligned}$$

where $\zeta_S(G,s)$ and $\zeta_H(G,s)$ are called the *zeta function of Sylow type* and *zeta function of Frobenius type*, respectively.

Equivalence relation on finite groups

We note that $\zeta(G,s)$ and $\zeta_S(G,s)$ are finite sums and that in particuler,

$$\zeta_S(G,s) = \sum_{x \in G} \frac{1}{|x|^s}.$$

Then from the fact $h_G(n) = \sum_{d|n} O_G(d)$, we have

$$\zeta_H(G,s) = \zeta_S(G,s)\zeta(s),$$

where $\zeta(s)$ is the Riemann zeta function. Firstly we shall show the following elementary proposition.

Proposition 1. *For all groups G_1 and G_2, the following conditions are equivalent* :

$$\begin{array}{llcll}
(1) & \zeta(G_1,s) & = & \zeta(G_2,s), & \\
(2) & \zeta_S(G_1,s) & = & \zeta_S(G_2,s), & \\
(3) & \zeta_H(G_1,s) & = & \zeta_H(G_2,s), & \\
(4) & s_{G_1}(n) & = & s_{G_2}(n) & \textit{for any } n \geq 1, \\
(5) & O_{G_1}(n) & = & O_{G_2}(n) & \textit{for any } n \geq 1, \\
(6) & h_{G_1}(n) & = & h_{G_2}(n) & \textit{for any } n \geq 1.
\end{array}$$

PROOF. It is obvious that (4) $\Longrightarrow$ (1), (5) $\Longrightarrow$ (2) and (6) $\Longrightarrow$ (3).

From the fact $O_G(n) = \varphi(n)s_G(n)$, one sees (4) $\Longleftrightarrow$ (5).

$\zeta_H(G,s) = \zeta_S(G,s)\zeta(s)$ implies the equivalence (2) $\Longleftrightarrow$ (3).

$h_G(n) = \sum_{d|n} O_G(d)$ and the Möbius inversion formula $O_G(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) h_G(d)$ imply the equivalence (5) $\Longleftrightarrow$ (6).

$\zeta(G,r) = (1, 2^r, \ldots, N^r)^t(s_G(1), s_G(2), \ldots, s_G(N))$, where $N = |G|$, implies

$$\begin{pmatrix} s_G(1) \\ s_G(2) \\ \vdots \\ s_G(N) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & N \\ \vdots & & & \vdots \\ 1 & 2^{N-1} & \cdots & N^{N-1} \end{pmatrix}^{-1} \begin{pmatrix} \zeta(G,0) \\ \zeta(G,1) \\ \vdots \\ \zeta(G,N-1) \end{pmatrix}.$$

Hence $\zeta(G_1,s) = \zeta(G_2,s)$ implies $s_{G_1}(n) = s_{G_2}(n)$ for any $1 \leq n \leq N$. Since $s_{G_1}(n) = s_{G_2}(n) = 0$ for any $n > N$, we see (1) $\Longrightarrow$ (4).
Similarly one can easily verify (2) $\Longrightarrow$ (5), which completes the proof.

As in [4], we will call G_1 and G_2 are *of the same order type* when G_1 and G_2 satisfy one of the above relations $(1), \ldots, (6)$, i.e., all of the relations, in which case we write $G_1 \sim G_2$. It is obvious that $\sim$ is an equivalence relation on the set of all the finite groups and $G_1 \cong G_2 \Longrightarrow G_1 \sim G_2$, but the converse is not true in general.

Let G be an abelian p-group,

$$G = (\mathbf{Z}/p^{e_1}\mathbf{Z})^{f_1} \times (\mathbf{Z}/p^{e_2}\mathbf{Z})^{f_2} \times \cdots \times (\mathbf{Z}/p^{e_r}\mathbf{Z})^{f_r},$$

where $1 \leq e_1 < e_2 < \cdots < e_r$. Evaluating $\log_p(h_G(p^x))$ we have shown in [4] that $h_G(p^x)$ determine $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ uniquely. Hence $G_1 \sim G_2 \Longleftrightarrow G_1 \cong G_2$ when G_1 and G_2 are finite abelian p-groups. Consequently we have shown $G_1 \sim G_2 \Longleftrightarrow G_1 \cong G_2$ when G_1 and G_2 are abelian groups (for details see Proposition 4 of [4]). Here we shall prove the following more precise result on abelian p-groups.

Proposition 2. *Let G_1 and G_2 are finite abelian $p-$groups. Then $\zeta_S(G_1,-1) = \zeta_S(G_2,-1)$ implies $G_1 \cong G_2$.*

PROOF. Let $G \cong (\mathbf{Z}/p^{e_1}\mathbf{Z})^{f_1} \times (\mathbf{Z}/p^{e_2}\mathbf{Z})^{f_2} \times \cdots \times (\mathbf{Z}/p^{e_r}\mathbf{Z})^{f_r}$. For the sake of simplicity, we denote $h_G(p^k) = p^{a(k)}$. Then by the definition of h_G, one sees $a(1) < a(2) < \cdots < a(e_r)$ and $a(k) = a(e_r)$ for any $k \geq e_r$. Then we have

$$\begin{aligned}
\zeta_S(G,-1) &= \sum_{k=0}^{e_r} O_G(p^k)p^k \\
&= \sum_{k=1}^{e_r}(h_G(p^k) - h_G(p^{k-1}))p^k + 1 \\
&= 1 - p + p^{a(1)+1} - p^{a(1)+2} + p^{a(2)+2} - p^{a(2)+3} + p^{a(3)+3} \\
&\quad + \cdots - p^{e_r+a(e_{r-1})} + p^{e_r+a(e_r)}.
\end{aligned}$$

Evaluate $\zeta_S(G,-1) \bmod p, p^2, p^3, \ldots$, we see $a(1), a(2), \ldots, a(e_r)$ are determined by $\zeta_S(G,-1)$. Thus we have

$$\begin{aligned}
\zeta_S(G_1,-1) = \zeta_S(G_2,-1) &\iff h_{G_1}(p^k) = h_{G_2}(p^k) \text{ for any } k \geq 0 \\
&\iff G_1 \sim G_2 \\
&\iff G_1 \cong G_2 (\text{see Proposition 4 of [4]}).
\end{aligned}$$

Let $m(G)$ be the arithmetic mean of the order of all the elements $x \in G$. Then one can easily verify that

$$m(G) = \frac{\zeta_S(G,-1)}{\zeta_S(G,0)},$$

where $\zeta_S(G,0) = |G|$. Hence we have the following corollary.

Corollary 1. *Let G_1 and G_2 are finite abelian $p-$groups. If $|G_1| = |G_2|$ and $m(G_1) = m(G_2)$, then we have $G_1 \cong G_2$.*

Arithmetically equivalent fields

Let k_1 and k_2 be algebraic number fields of finite degree. We denote the Dedekind zeta functions of k_1 and k_2 by $\zeta_{k_1}(s)$ and $\zeta_{k_2}(s)$, respectively. Then k_1 and k_2 are called *arithmetically equivalent* when $\zeta_{k_1}(s) = \zeta_{k_2}(s)$, in which case we write $k_1 \sim k_2$. It is obvious that if k_1 and k_2 are conjugate over Q, then $\zeta_{k_1}(s) = \zeta_{k_2}(s)$. We note that the first example of k_1 and k_2 which are arithmetically equivalent but not conjugate over Q was given by F. Gassmann [2] in 1926.

Let K be a Galois extension of Q with $k_1 \subset K$ and $k_2 \subset K$. We denote the Galois group $Gal(K/Q)$ by G and the corresponding subgroups $Gal(K/k_1)$ and

$Gal(K/k_2)$ by G_1 and G_2, respectively. Then the following proposition is well known.

Proposition 3. *The following conditions are equivalent:*

(1) *k_1 and k_2 are arithmetically equivalent.*
(2) *For every prime p, the collection of degrees of the prime ideal factors p in k_1 equals to the collection of degrees of the prime ideal factors in k_2.*
(3) *For every element $\sigma \in G$, $\#[C_\sigma \cap G_1] = \#[C_\sigma \cap G_2]$, where C_σ is the class of conjugate elements of σ in G.*

Following [6], we will say that G_1 and G_2 are *Gassmann equivalent* in G when $G_1, G_2 < G$ satisfy the condition (3) of Proposition 3, in which case we will write $G_1 \sim_G G_2$. We will write $G_1 \sim_C G_2$ when G_1 and G_2 are conjugate in G.

For any $H < G$, we will denote the family of all the conjugate subgroups of H in G by $[H]$, i.e.,

$$[H] = \{\sigma H \sigma^{-1} | \sigma \in G\}.$$

Put

$$C(G) = \{[H] | H < G\}.$$

Suppose $G_1 \in [H_1]$, $G_2 \in [H_2]$ and $G_1 \sim_G G_2$. From the fact $\sim_C \Longrightarrow \sim_G$, any $G_1' \in [H_1]$ and $G_2' \in [H_2]$ satisfy $G_1' \sim_G G_2'$. Thus we may consider $\sim_G$ to be an equivalence relation on $C(G)$, that is,

$$[H_1] \sim_G [H_2] \Longleftrightarrow H_1 \sim_G H_2.$$

Let $G(N)$ be the set of all the finite groups of order N. It is well known that any $H \in G(N)$ can be considered as a subgroup of the symmetric group S_N by the left regular representation. For the sake of the completeness, we will recall the definition of the left regular representation.

Let $X = \{x_1, \ldots, x_N\}$ be an ordering of all the elements in H. Then $xx_k = x_{x(k)}$ for k $(1 \le k \le N)$ determines a regular representation

$$\varphi_X : x \longrightarrow \begin{pmatrix} 1 & \ldots & N \\ x(1) & \ldots & x(N) \end{pmatrix} \in S_N$$

and $\varphi_X(H) < S_N$.

The regular representation may depend on the ordering X as follows. Let $Y = \{y_1, \ldots, y_N\}$ be another ordering of the elements in H, i.e., $y_k = x_{\sigma(k)}$ $(1 \le k \le N)$ for some $\sigma \in S_N$. Then we have

$$xy_k = xx_{\sigma(k)} = x_{x(\sigma(k))} = y_{\sigma^{-1}x(\sigma(k))} \ (1 \le k \le N).$$

So for any $x \in H$, the regular representation satisfies

$$\varphi_Y(x) = \sigma^{-1}\varphi_X(x)\sigma \in S_N.$$

Thus we have $\varphi_Y(H) = \sigma^{-1}\varphi_X(H)\sigma$, which means that with respect to the ordering of the elements, the regular representation determines a map from $G(N)$ to the set of conjugacy classes $C(S_N)$. We will denote this map by φ, i.e.,

$$\varphi(H) = [\varphi_X(H)],$$

where $X = \{x_1, \ldots, x_N\}$ is an ordering of the elements of H.

It is obvious that $H_1 \cong H_2$ when $\varphi(H_1) = \varphi(H_2) \in C(S_N)$. Conversely we can see that $\varphi(H_1) = \varphi(H_2)$ when $H_1 \cong H_2$ as follows. Let ψ be an isomorphism from H_1 to H_2. Take the orderings $X = \{x_1, \ldots, x_N\}$ of H_1 and $Y = \{\psi(x_1), \ldots, \psi(x_N)\}$ of H_2. Put $xx_k = x_{x(k)}$ for $1 \leq k \leq N$. Then $\psi(x)\psi(x_k) = \psi(xx_k) = \psi(x_{x(k)})$ implies $\varphi_X(H_1) = \varphi_Y(H_2)$. Thus we have shown

$$\varphi(H_1) = [\varphi_X(H_1)] = [\varphi_Y(H_2)] = \varphi(H_2).$$

Hence we have shown that φ induces the following injective map

$$\bar{\varphi} : \{G(N)/\cong\} \longrightarrow C(S_N).$$

Let $\bar{H}$ be the isomorphism class of H in $\{G(N)/\cong\}$. Since $\cong \Longrightarrow \sim$, $\sim$ may be considered as an equivalence relation on $\{G(N)/\cong\}$, i.e.,

$$\bar{H}_1 \sim \bar{H}_2 \Longleftrightarrow H_1 \sim H_2.$$

Let X be an ordering of $H \in G(N)$. When $|x| = m$, one knows $\varphi_X(x)$ is of type $m + m + \cdots + m$ in S_N. Thus we have

$$\#[C_\sigma \cap \varphi_X(H)] = \begin{cases} O_H(m) & \text{if there exist } x \in H \text{ with } |x| = m, \\ & \text{and } \sigma \text{ is of type } m + m + \cdots + m, \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\begin{aligned} [H_1] \sim_G [H_2] &\Longleftrightarrow O_{H_1}(n) = O_{H_2}(n) \quad \text{for any } n \geq 0 \\ &\Longleftrightarrow \bar{H}_1 \sim \bar{H}_2. \end{aligned}$$

Theorem. *With the above notations, the map*

$$\bar{\varphi} : \{G(N)/\cong\} \longrightarrow C(S_N)$$

is injective and

$$\bar{\varphi}(\bar{H}_1) \sim_G \bar{\varphi}(\bar{H}_2) \Longleftrightarrow \bar{H}_1 \sim \bar{H}_2.$$

Let K be a Galois extension of $\boldsymbol{Q}$ with Galois group $Gal(K/\boldsymbol{Q}) \cong S_N$. Let $F(N)$ be the set of intermediate fields of K corresponding to the set of subgroups $\varphi(G(N))$. Then we have the following corollaries.

Corollary 2. *Let $H_1, H_2 \in G(N)$ and X_i be some orderings for $i = 1, 2$. We denote the fixed fields of $\varphi_{X_1}(H_1)$ and $\varphi_{X_2}(H_2)$ by k_1 and k_2 $(\in F(N))$, respectively. Then*

$$\begin{aligned} k_1 \text{ and } k_2 \text{ are conjugate over } \boldsymbol{Q} &\iff \varphi_{X_1}(H_1) \sim_C \varphi_{X_2}(H_2) \text{ in } S_N \\ &\iff \varphi(H_1) = \varphi(H_2) \\ &\iff H_1 \cong H_2, \end{aligned}$$

and

$$\begin{aligned} k_1 \sim k_2 &\iff \varphi_{X_1}(H_1) \sim_G \varphi_{X_2}(H_2) \text{ in } S_N \\ &\iff H_1 \sim H_2. \end{aligned}$$

Corollary 3. *Let $H_1, H_2 \in G(N)$ and k_1 and k_2 are corresponding subgroups of S_N as above. Then*

$$\begin{aligned} \zeta_{k_1}(s) = \zeta_{k_2}(s) &\iff \zeta(H_1, s) = \zeta(H_2, s) \\ &\iff \zeta_S(H_1, s) = \zeta_S(H_2, s) \\ &\iff \zeta_H(H_1, s) = \zeta_H(H_2, s). \end{aligned}$$

Remark. It is interesting to consider the difference between $\cong$ and $\sim$ in $G(N)$, because the difference is exactly the number of arithmetical equivalent fields which are not conjugate over $\boldsymbol{Q}$ as in the above sense. Let p be an odd prime. In the papers [4] and [8], we have estimated the number

$$a(n) = \#\{\{H \sim (\mathbf{Z}/p\mathbf{Z})^n\}/\cong\}.$$

Since our estimate for $a(n)$ is not good enough, it is expected that sharper estimates can be obtained with methods like in [7].

Acknowledgement. This paper was written during the author's scholarship stay at Université Laval. The author expresses his heartily thanks for the kind hospitality to the staff of Département de Mathématiques et de Statistique. He is very grateful to Professor Claude Levesque for his continuous encouragement.

References

[1] W. S. Burnside, Theory of Groups of Finite Orders, Cambridge Univ. Press, Cambridge 1911.

[2] F. Gassmann, Bemerkungen zur vorstehenden Arbeit von Hurwitz, *Math. Zeit.*, **25** (1926), 665-675.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers (5th ed.), Clarendon Press, Oxford 1979.

[4] S. Katayama, On zeta functions associated to finite groups, preprint.

[5] N. Klingen, Arithmetical Similarities, Clarendon Press, Oxford 1998.

[6] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, *J. Number Theory.* **9** (1977), 242–260.

[7] C. Sims, Enumerating p-groups, *Proc. London Math. Soc.* (3), **15** (1965), 151-166.

[8] T. Tamai, On the constuction of the arithmetically equivalent fields, Master Thesis (2001), Tokushima University (in Japanese).

[9] T. Yoshida, Zeta functions related with theorems of Sylow and Frobenius, Algebraic Combinatories, *RIMS* **768** (1991), pp1–15 (in Japanese).