Spectra of Vertex-Transitive Graphs and Hecke Algebras of Finite Groups II

Michihiko HASHIZUME and Yoshiyuki MORI
Department of Applied Mathematics, Faculty of Science
Okayama University of Science
Ridaicho 1-1, Okayama 700, Japan
(Received October 7, 1996)

1 Introduction

This paper is a continuation of our paper[2]. Here we consider the two families of Hecke algebras of certain finite affine transformation groups. We shall prove that those Hecke algebras are commutative. We shall also determine both the multiplication tables and the character tables with respect to the canonical basis of our Hecke algebras explicitly.

2 The first example

Let $\boldsymbol{Z}$ be the ring of integers and $\boldsymbol{N}$ be the set of natural numbers. Fix a prime p and $n \in \boldsymbol{N}$. Let $\boldsymbol{Z}/p^n$ be the ring of integers mod. p^n and $(\boldsymbol{Z}/p^n)^\times$ be the multiplicative group of $\boldsymbol{Z}/p^n$. Note that $|\boldsymbol{Z}/p^n| = p^n$ and $|(\boldsymbol{Z}/p^n)^\times| = \varphi(p^n) = p^{n-1}(p-1)$, where φ is Euler's function. Consider the $(\boldsymbol{Z}/p^n)^\times$ orbits in $\boldsymbol{Z}/p^n$. It is easy to see that the orbit decomposition of $\boldsymbol{Z}/p^n$ is given by

$$\boldsymbol{Z}/p^n = \{0\} \cup \bigcup_{k=0}^{n-1} (\boldsymbol{Z}/p^n)^\times \cdot p^k \tag{1}$$

where

$$(\boldsymbol{Z}/p^n)^\times \cdot p^k = \{up^k ; u \in (\boldsymbol{Z}/p^{n-k})^\times\} (0 \leq k \leq n-1). \tag{2}$$

The isotropy subgroup of $(\boldsymbol{Z}/p^n)^\times$ at p^k is given by

$$(\boldsymbol{Z}/p^n)^\times_{p^k} = \{1 + bp^{n-k} ; b \in \boldsymbol{Z}/p^k\}. \tag{3}$$

We define a multiplication rule on the direct product $G = (\boldsymbol{Z}/p^n)^\times \times \boldsymbol{Z}/p^n$ by

$$(a, b)(a', b') = (aa', b + ab'). \tag{4}$$

Then G becomes a finite group of order $p^{2n-1}(p-1)$, whose unit element is $(1, 0)$ and the inverse of (a, b) is $(a^{-1}, -a^{-1}b)$. Put $H = \{(y, 0) ; y \in (\boldsymbol{Z}/p^n)^\times\}$ and $N = \{(1, x) ; x \in \boldsymbol{Z}/p^n\}$. Then H is a subgroup of G isomorphic to $(\boldsymbol{Z}/p^n)^\times$ and N is a normal subgroup of G isomorphic to $\boldsymbol{Z}/p^n$. Since

$$(y, x) = (1, x)(y, 0) = (y, 0)(1, y^{-1}x), \tag{5}$$

we have $G = NH = HN$. Let G/H be the coset space of G with respect to H. Then it follows from (5) that $G/H = \{(1, x)H; x \in \boldsymbol{Z}/p^n\}$. Let $H\backslash G/H$ be the double coset space of G with respect to H. Then it follows from (5) that

$$H(y, x)H = H(1, x)H = H(1, ax)H, \ a \in (\boldsymbol{Z}/p^n)^{\times}.$$

Consequently we conclude from (1) that

$$H\backslash G/H = \{H, D_k = H(1, p^k)H(0 \leq k \leq n-1)\} \tag{6}$$

and from (2)

$$D_k = H(1, p^k)H = \bigcup_{u \in (Z/p^{n-k})^{\times}} (1, up^k)H(0 \leq k \leq n-1). \tag{7}$$

Hence the number of H-cosets in D_k is equal to $\varphi(p^{n-k}) = p^{n-k-1}(p-1)$. Let $\mathcal{H}$ be the Hecke algebra of G with respect to H. It is a subalgebra of the group algebra $\boldsymbol{C}G$ defined by $\mathcal{H} = e\boldsymbol{C}Ge$, where $e \in \boldsymbol{C}G$ is given by

$$e = |H|^{-1} \sum_{h \in H} h = \varphi(p^n)^{-1} \sum_{a \in (Z/p^n)^{\times}} (a, 0). \tag{8}$$

Define $\varepsilon_k \in \mathcal{H}(0 \leq k \leq n-1)$ by

$$\varepsilon_k = |H|^{-1} \sum_{g \in D_k} g.$$

It is known[2] that

$$\varepsilon_k = \varphi(p^{n-k})e(1, p^k)e(0 \leq k \leq n-1), \tag{9}$$

and $\{e, \varepsilon_k(0 \leq k \leq n-1)\}$ forms a basis of $\mathcal{H}$. Since $-1 \equiv p^n - 1 \in (\boldsymbol{Z}/p^n)^{\times}$, it follows that $D_k^{-1} = H(1, -p^k)H = H(1, p^k)H = D_k$. Therefore $\mathcal{H}$ is a commutative algebra[3].

Theorem 1. The Hecke algebra $\mathcal{H}$ is an $(n+1)$-dimensional commutative semisimple algebra, whose multiplication table is given by

$$e^2 = e, \ e\varepsilon_m = \varepsilon_m(0 \leq m \leq n-1) \tag{10}$$

$$\varepsilon_l\varepsilon_m = \varphi(p^{n-m})\varepsilon_l(0 \leq l < m \leq n-1) \tag{11}$$

$$\varepsilon_m^2 = \varphi(p^{n-m})(e + \sum_{m+1 \leq j \leq n-1} \varepsilon_j) + p^{n-m-1}(p-2)\varepsilon_m(0 \leq m \leq n-1). \tag{12}$$

Proof. It is enough to show (11) and (12). From (9), we have

$$\varepsilon_l\varepsilon_m = \varphi(p^{n-l})\varphi(p^{n-m})e(1, p^l)e(1, p^m)e.$$

Using (8), we have

$$(1, p^l)e(1, p^m) = \varphi(p^n)^{-1} \sum_{a \in (Z/p^n)^{\times}} (a, p^l(1 + ap^{m-l})).$$

Since $m > l$ and $1 + ap^{m-l} \in (\boldsymbol{Z}/p^n)^{\times}$, it follows that

$$(a, p^l(1+ap^{m-l})) = (1+ap^{m-l}, 0)(1, p^l)(a(1+ap^{m-l})^{-1}, 0)$$

and hence

$$e(1, p^l)e(1, p^m)e = \varphi(p^n)^{-1} \sum_{a\in(Z/p^n)^\times} e(1,p^l)e$$
$$= e(1, p^l)e.$$

Consequently we have

$$\varepsilon_l\varepsilon_m = \varphi(p^{n-m})\varepsilon_l \ for \ 0 \leq l < m \leq n-1.$$

It follows from (8), (9)

$$e_m^2 = \varphi(p^{n-m})^2 e(1, p^m)e(1, p^m)e$$
$$= \varphi(p^{n-m})^2\varphi(p^n)^{-1} \sum_{a\in(Z/p^n)^\times} e(1, p^m(1+a))e.$$

Note that

$$1+(\boldsymbol{Z}/p^n)^\times = \{0\} \cup \bigcup_{k=1}^{n-1}(\boldsymbol{Z}/p^n)^\times \cdot p^k \cup ((1+(\boldsymbol{Z}/p^n)^\times) \cap (\boldsymbol{Z}/p^n)^\times)$$

and

$$|(1+(\boldsymbol{Z}/p^n)^\times) \cap (\boldsymbol{Z}/p^n)^\times| = p^{n-1}(p-2).$$

The sum $\sum_{a\in(Z/p^n)^\times} e(1, p^m(1+a))e$ is given by

$$e+ \sum_{1\leq k\leq n-1} \sum_{u\in(Z/p^{n-k})^\times} e(1, p^{m+k}u)e + \sum_{v\in(1+(Z/p^n)^\times)\cap(Z/p^n)^\times} e(1, p^m v)e,$$

which equals

$$e+ \sum_{1\leq k\leq n-1} \varphi(p^{n-k})e(1, p^{m+k})e + p^{n-1}(p-2)e(1, p^m)e.$$

Since $p^{m+k} \equiv 0$ for $n-m \leq k \leq n-1$, it can be written as

$$(1+ \sum_{n-m\leq k\leq n-1} \varphi(p^{n-k}))e \sum_{m+1\leq j\leq n-1} p^m\varphi(p^{n-j})e(1, p^j)e + p^{n-1}(p-2)e(1, p^m)e.$$

Since the coefficient of e is p^m, the above sum is equal to

$$p^m e + p^m \sum_{m+1\leq j\leq n-1} \varepsilon_j + p^{n-1}(p-2)\varphi(p^{n-m})^{-1}\varepsilon_m.$$

Applying $\varphi(p^{n-m})^2\varphi(p^n)^{-1} = \varphi(p^{n-m})/p^m$, we have

$$\varepsilon_m^2 = \varphi(p^{n-m})(e + \sum_{m+1\leq j\leq n-1} \varepsilon_j) + p^{n-m-1}(p-2)\varepsilon_m. \quad //$$

From Theorem 1, we conclude that all the irreducible representations are 1-dimensional and there are exactly (n+1) irreducible characters of $\mathcal{H}$.

Theorem 2. Let $\hat{\mathcal{H}}$ be the set of all irreducible characters of $\mathcal{H}$. Then

$$\hat{\mathcal{H}} = \{1_{\mathcal{H}}, \chi_k(0 \leq k \leq n-1)\}$$

where

$$1_{\mathcal{H}}(e) = 1, 1_{\mathcal{H}}(\varepsilon_m) = \varphi(p^{n-m})$$

and

$$\chi_k(e) = 1,\ \chi_k(\varepsilon_m) = 0 (0 \leq m \leq k-1),\ \chi_k(\varepsilon_k) = -p^{n-k-1},$$
$$\chi_k(\varepsilon_m) = \varphi(p^{n-m})(k+1 \leq m \leq n-1).$$

Proof. Let χ be an irreducible character of $\mathcal{H}$ and put $\chi(\varepsilon_m) = \lambda_m (0 \leq m \leq n-1)$. Since $\varepsilon_{n-1}^2 = \varphi(p)e + (p-2)\varepsilon_{n-1}$, we have $\lambda_{n-1}^2 = \varphi(p) + (p-2)\lambda_{n-1}$ and hence $\lambda_{n-1} = -1$ or $\varphi(p)$. Since $\varepsilon_m\varepsilon_{n-1} = \varphi(p)\varepsilon_m (0 \leq m \leq n-2)$ and $\varepsilon_{n-2}^2 = \varphi(p^2)(e+\varepsilon_{n-1}) + p(p-2)$ ε_{n-2}, we conclude that $\lambda_m = 0 (0 \leq m \leq n-2)$ if $\lambda_{n-1} = -1$ and $\lambda_{n-2} = -p$ or $\varphi(p^2)$ if $\lambda_{n-1} = \varphi(p)$. Therefore if $\chi(\varepsilon_{n-1}) = -1$ then $\chi = \chi_{n-1}$. Assume $\lambda_{n-1} = \varphi(p)$ and $\lambda_{n-2} = -p$. Then $\varepsilon_m\varepsilon_{n-2} = \varphi(p^2)\varepsilon_m (0 \leq m \leq n-3)$ implies $\lambda_m = 0 (0 \leq m \leq n-3)$. Therefore if $\chi(\varepsilon_{n-1}) = \varphi(p)$ and $\chi(\varepsilon_{n-2}) = -p$ then $\chi = \chi_{n-2}$. Assume $\lambda_{n-1} = \varphi(p)$ and $\lambda_{n-2} = \varphi$ (p^2). Then $\varepsilon_{n-3}^2 = \varphi(p^3)(e+\varepsilon_{n-2}+\varepsilon_{n-1}) + p^2(p-2)\varepsilon_{n-3}$ implies that $\lambda_{n-3} = -p^2$ or $\varphi(p^3)$. If $\lambda_{n-3} = -p^2$ we have $\chi = \chi_{n-3}$. Continuing this process, we conclude that χ is equal to either $\chi_k (0 \leq k \leq n-1)$ or $1_{\mathcal{H}}$.

3 The second example

Let $\boldsymbol{F}_q$ be the finite field with q elements and $\boldsymbol{F}_q^{\times}$ be the multiplicative group of $\boldsymbol{F}_q$. Then $\boldsymbol{F}_q^{\times}$ is a cyclic group of order $q-1$. Let $a \in \boldsymbol{F}_q^{\times}$, whose order is m. Put $l = (q-1)/m$. We denote by $\langle a \rangle$ the cyclic subgroup of $\boldsymbol{F}_q^{\times}$ generated by a. Consider the $\langle a \rangle$ orbits in $\boldsymbol{F}_q$. It is easy to show that there are exactly $l+1$ orbits of $\langle a \rangle$ in $\boldsymbol{F}_q$. We write them by $\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_l$ where $\mathcal{O}_j = \langle a \rangle \cdot b_j (0 \leq j \leq l)$ with the set of representatives of orbits $\{b_0 = 0, b_1 = 1, b_2, \ldots, b_l\}$. Note that $\mathcal{O}_0 = \{0\}$ and $|\mathcal{O}_j| = m (1 \leq j \leq l)$. We define a multiplication rule on the direct product $G = \langle a \rangle \times \boldsymbol{F}_q$ by

$$(y, x)(y', x') = (yy', x+yx').$$

Then G is a finite group of order mq. Put $H = \{(y, 0); y \in \langle a \rangle\}$ and $N = \{(1, x); x \in \boldsymbol{F}_q\}$. Then H is a subgroup of G isomorphic to $\langle a \rangle$ and N is a normal subgroup of G isomorphic to $\boldsymbol{F}_q$. Furthermore $G = HN = NH$. Let G/H be the coset space of G with respect to H.Then $G/H = \{(1, x)H; x \in \boldsymbol{F}_q\}$. Let $H\backslash G/H$ be the double coset space of G with respect to H. Since $H(y, x)H = H(1, x)H = H(1, ux)H$ for $u \in \langle a \rangle$, it follows that

$$H\backslash G/H = \{D_j = H(1, b_j)H; 0 \leq j \leq l\}$$

and

$$D_j = \bigcup_{x \in \mathcal{O}_j} (1, x)H (0 \leq j \leq l).$$

Define e and $\varepsilon_j \in \boldsymbol{C}G (1 \leq j \leq l)$ by

$$e = m^{-1} \sum_{0 \leq k \leq m-1} (a^k, 0),$$
$$\varepsilon_j = me(1, b_j)e(1 \leq j \leq l).$$

Put $\mathcal{H} = eCGe$. Then $\mathcal{H}$ is the Hecke algebra of G relative to H. Furthermore $\{e, \varepsilon_j (1 \leq j \leq l)\}$ forms a basis of $\mathcal{H}$.

Theorem 3. Let $\mathcal{H}$ be the Hecke algebra of G relative to H. Then $\mathcal{H}$ is an $(l+1)$-dimensional commutative semisimple algebra, whose multiplication table is given by

$$e^2 = e, e\varepsilon_j = \varepsilon_j (1 \leq j \leq l),$$
$$(*) \quad \varepsilon_i \varepsilon_j = mc_{ij}^0 e + \sum_{1 \leq k \leq l} c_{ij}^k \varepsilon_k (1 \leq i, j \leq l),$$

where we put

$$c_{ij}^k = |(b_i + \mathcal{O}_j) \cap \mathcal{O}_k| (0 \leq k \leq l).$$

Proof, Let $1 \leq i, j \leq l$. Since

$$(1, b_i)e(1, b_j) = m^{-1} \sum_{0 \leq t \leq m-1} (1, b_i + a^t b_j)(a^t, 0),$$

it follows that

$$\varepsilon_i \varepsilon_j = m \sum_{0 \leq t \leq m-1} e(1, b_i + a^t b_j)e.$$

It can be written as

$$\varepsilon_i \varepsilon_j = m \sum_{0 \leq k \leq l} c_{ij}^k e(1, b_k)e.$$

This means $(*)$. Define the map $f: b_i + \mathcal{O}_j \to b_j + \mathcal{O}_i$ by $f(b_i + a^t b_j) = b_j + a^{m-t} b_i (0 \leq t \leq m-1)$. Then f is a bijection. In particular f induces a bijection from $(b_i + \mathcal{O}_j) \cap \mathcal{O}_k$ to $(b_j + \mathcal{O}_i) \cap \mathcal{O}_k$. Hence $c_{ij}^k = c_{ji}^k$, which shows the commutativity of $\mathcal{H}$. //

To determine the set of all irreducible characters of $\mathcal{H}$, we first decide the character table of G. Let $[G]$ and $\widehat{G}$ be the set of all conjugacy classes of G and the set of all irreducible characters of G respectively. Simple caluculation shows that

$$[G] = \{[1, 0] = \{(1, 0)\}, [1, b_i] = \{(1, x); x \in \mathcal{O}_i\} (1 \leq i \leq l),$$
$$[a^k, 0] = \{(a^k, x); x \in \boldsymbol{F}_q\} (1 \leq k \leq m-1)\}$$

On the other hand, $\widehat{G}$ can be determined by Mackey's theorem[1] in the following manner. Let ψ be the nontrivial additive character of $\boldsymbol{F}_q$. For $b \in \boldsymbol{F}_q$, we put $\psi_b(x) = \psi(bx) (x \in \boldsymbol{F}_q)$. Let $\widehat{N}$ be the set of all irreducible characters of N. Since N is isomorphic to $\boldsymbol{F}_q$, it follows that $\widehat{N} = \{\psi_b; b \in \boldsymbol{F}_q\}$. The set $\widehat{N}/\langle a \rangle$ of $\langle a \rangle$ orbits in $\widehat{N}$ is given by $\widehat{N}/\langle a \rangle = \{\psi_{b_i}; 0 \leq i \leq l\}$. Let χ_i be the induced character $ind_N^G(\psi_{b_i}) (1 \leq i \leq l)$. On the other hand, the set of all irreducible characters $\langle a \rangle^{\widehat{}}$ of $\langle a \rangle$ is given by $\langle a \rangle^{\widehat{}} = \{\sigma_j;$

$0 \leq j \leq m-1\}$, where

$$\sigma_j(a^k) = e^{2\pi ijk/m}(0 \leq k \leq m-1).$$

From Mackey's theorem, we conclude

$$\hat{G} = \{\sigma_j; 0 \leq j \leq m-1\} \cup \{\chi_i; 1 \leq i \leq l\},$$

where we define the character σ_j of G by $\sigma_j\,(y, x) = \sigma_j(y)$. The character table of G is given by

	$[1, 0]$	$[1, b_j](1 \leq j \leq l)$	$[a^k, 0](1 \leq k \leq m-1)$
$\sigma_j(0 \leq j \leq m-1)$	1	1	$e^{2\pi ijk/m}$
$\chi_i(1 \leq i \leq l)$	m	$\sum_{0 \leq k \leq m-1} \psi(a^k b_i b_j)$	0

It can be easily seen that the irreducible constituents of $ind_H^G(1_H)$ are $1_G = \sigma_0$ and χ_i $(1 \leq i \leq l)$. They yield all the irreducible characters of $\mathcal{H}$ in the following way[2]. Let χ be an irreducible constituent of $ind_H^G\,(1_H)$. Then by putting

$$\chi^{\mathcal{H}}(\varepsilon_j) = |H|^{-1} \sum_{C \in [G]} |C \cap D_j| \chi(C),$$

we get the irreducible character $\chi^{\mathcal{H}}$ of $\mathcal{H}$. Finally the character table of $\mathcal{H}$ is given by

	e	$\varepsilon_j(1 \leq j \leq l)$
$1 = \sigma_0^{\mathcal{H}}$	1	m
$\chi_i(1 \leq i \leq l)$	1	$\sum_{0 \leq k \leq m-1} \psi(a^k b_i, b_j)$

References

1) C. W. Curtis nd I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, New York, 1962.
2) M. Hashizume and Y. Mori, Spectra of Vertex-Transitive Graphs and Hecke Algebras of Finite Groups, The Bull. of the Okayama Univ. of Sci., No. 31 A (1996) 7-15.
3) Y. Mori, Structure of Hecke Algegras of Finite Groups and their Character Tables, Master Thesis, Graduate School of Okayama University of Science, 1996.