On the group algebras of metacyclic groups over algebraic number fields

By Toshihiko YAMADA
(Comm. by Y. Kawada)

1. Introduction

Let G be a finite group, and K an algebraic number field of finite degree over the rational number field $\boldsymbol{Q}$. The group algebra $K[G]$ of G with regard to K is a direct sum of simple algebras A_i:

$$K[G]=A_1 \oplus A_2 \oplus \cdots \oplus A_h . \tag{1}$$

Each A_i is isomorphic to a complete matric algebra $M_{n_i}(D_i)$ over a division algebra D_i, whose center is an extension field K_i of finite degree r_i over K. If m_i^2 is the degree of D_i over K_i, A_i has the rank $r_i n_i^2 m_i^2$ over K. By a K-representation of G, we mean a matrix representation, whose coefficients belong to K. Then the simple algebras $A_1, A_2, \cdots, A_h$ in (1) are in one-to-one correspondence to the irreducible K-representations $T_1, T_2, \cdots, T_h$. If $\boldsymbol{C}$ is the field of complex numbers, then T_i breaks up in $\boldsymbol{C}$ into r_i distinct absolutely irreducible representations $U_1^{(i)}, U_2^{(i)}, \cdots, U_{r_i}^{(i)}$, each appearing with the same multiplicity m_i. Thus, if the characters of $U_\nu^{(i)}$ are denoted by $\chi_\nu^{(i)}$, the character of T_i is given by $m_i(\chi_1^{(i)}+\chi_2^{(i)}+\cdots+\chi_{r_i}^{(i)})$. The number m_i is called the Schur index of each of the characters $\chi_1^{(i)}, \chi_2^{(i)}, \cdots, \chi_{r_i}^{(i)}$ and of the simple component A_i in (1). The r_i characters $\chi_1^{(i)}, \cdots, \chi_{r_i}^{(i)}$ form a full family of absolutely irreducible characters which are algebraically conjugate with regard to K, and $K(\chi_1^{(i)})=\cdots=K(\chi_{r_i}^{(i)})$, where $K(\chi_\nu^{(i)})$ is the field obtained from K by adjunction of all values $\chi_\nu^{(i)}(a)$, $a \in G$. The simple component A_i of $K[G]$ which corresponds to T_i is isomorphic to the enveloping algebras of $U_\nu^{(i)}$ with respect to K:

$$A_i \simeq \mathrm{env}_K(U_\nu^{(i)}) , \quad 1 \leqslant \nu \leqslant r_i . \tag{2}$$

The center K_i of A_i is isomorphic over K to the field $K(\chi_\nu^{(i)})$.

It is well known that every simple algebra over an algebraic number field is a cyclic algebra. Therefore it is desirable that each simple component of a group algebra is expressed as a cyclic algebra and its Schur index is determined. In this paper we solve the problem for metacyclic groups satisfying a condition. In this connection, the structures of group algebras of nilpotent groups have been completely determined by Roquette [8].

Here we give a brief account of our results. Let G be a metacyclic group containing a cyclic normal subgroup $H=\langle\omega\rangle$ of order m and with a cyclic factor group $G/H=\langle\sigma H\rangle$ of order s. If G is a split extension of H by G/H, (for instance if $(m, s)=1$, an extension must split), all the absolutely irreducible representations of G are explicitly determined and their number is counted (Theorem 1). Each of them is induced from a one-dimensional representation of a certain subgroup of G.

Notation being as above, suppose that $(m, s)=1$. Then the enveloping algebra with respect to $\boldsymbol{Q}$ of every irreducible representation of G is definitely expressed as a cyclic algebra (Theorem 2), so that the structure of $\boldsymbol{Q}[G]$ is determined (Theorem 2′). This result is obtained directly from the structure of the matrices of each irreducible representation.

The Schur index (with respect to $\boldsymbol{Q}$) of an irreducible representation U of G is the index of the central simple algebra $\mathrm{env}_{\boldsymbol{Q}}(U)$ over its center $Q(\chi)$, χ being the character of U. Recall that the index of a cyclic algebra over an algebraic number field can be decided by computing the norm residue symbol. Consequently if G is a metacyclic group satisfying $(m, s)=1$ as before, it is necessary to calculate with norm residue symbols in order to determine the Schur indices of the irreducible representations of G. By making use of the class field theory, the computation is carried out, and the local indices of $\mathrm{env}_{\boldsymbol{Q}}(U)$ for each irreducible representation U of G are exactly decided (Theorem 3). Thus we find Schur indices of all the irreducible representations of G (Theorem 4). The obtained formula is apparently complicated, but using this, we can easily compute the Schur indices for any given group G.

Brauer [2] has reduced the question of the Schur indices to the determination of the indices for $\boldsymbol{Q}$-elementary groups. When p is a given prime number, a group G is said to be a $\boldsymbol{Q}$-elementary group (at p) if G is a semi-direct product $G=\langle\omega\rangle P$, where $\langle\omega\rangle$ is a cyclic normal subgroup of G of order m, P a p-group such that $(p, m)=1$. It is clear that P is a p-Sylow subgroup of G. Now a $\boldsymbol{Q}$-elementary group (at p) whose p-Sylow subgroups are cyclic is one of aforesaid metacyclic groups. Therefore we have settled the problem of the Schur indices for all the $\boldsymbol{Q}$-elementary groups whose p-Sylow subgroups are cyclic.

Finally we shall deal with application of our results to number theory. In Appendix we examine the l-adic representations of certain automorphism groups of the Davenport-Hasse curves. Then for every characteristic $p>2$, we find examples where the Artin representation (cf. Serre [9]) cannot be realized over the p-adic number field $\boldsymbol{Q}_p$.

Notation and Terminology. As usual $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ denote respectively the ring of rational integers, the rational number field, the real number field, the complex number field. If p is a prime number, $\boldsymbol{Q}_p$ denotes the field of p-adic numbers. For a set M, $\#(M)$ is the cardinality of M. For a field K, $K^\times = K - \{0\}$. For a natural number n, the multiplicative group of integers modulo n is denoted by $(\boldsymbol{Z} \bmod n)^\times$. If an integer r is relatively prime to n, the order of $r \pmod n$ in the group $(\boldsymbol{Z} \bmod n)^\times$ is said simply as the order of $r \pmod n$. If a field K is a Galois extension of a field k, then $\mathfrak{G}(K/k)$ is its Galois group. When we say that a representation of a finite group G is irreducible, we always mean that it is absolutely irreducible.

2. The irreducible representations of metacyclic groups

Let G be a metacyclic group containing a cyclic normal subgroup H of order m and with a cyclic factor group G/H of order s. Throughout this paper we assume that G is a split extension of H by G/H, so that G has two generators ω and σ satisfying the relations

$$(1) \qquad \omega^m = 1 , \quad \sigma^{-1}\omega\sigma = \omega^r , \quad \sigma^s = 1 .$$

In the multiplicative group of $(\boldsymbol{Z} \bmod m)^\times$, r has order u. We always assume that $u \neq 1$, because in the case $u = 1$, G is abelian. The integers m, s, r, u must satisfy the following conditions:

$$(2) \qquad (m, r) = 1 , \quad u | s .$$

Finally, we observe that the elements of G can be expressed uniquely in the form

$$(3) \qquad \omega^\nu \sigma^\mu , \quad 0 \leqq \nu \leqq m-1 , \quad 0 \leqq \mu \leqq s-1 .$$

For any divisor t of u, ω and σ^t generate the normal subgroup H_t of G:

$$(4) \qquad H_t = \left\{ \omega^\nu \sigma^{t\mu} ; \ 0 \leqq \nu \leqq m-1, \ 0 \leqq \mu \leqq \frac{s}{t} - 1 \right\} .$$

H_t is a metacyclic group containing the cyclic normal subgroup $\langle \omega \rangle$ of order m and with the cyclic factor group $H_t/\langle \omega \rangle \simeq \langle \sigma^t \rangle$ of order $\frac{s}{t}$, such that

$$(5) \qquad \sigma^{-t}\omega\sigma^t = \omega^{r^t} .$$

The following Lemma is easily proved:

LEMMA 1. *The commutator group $[H_t, H_t]$ of H_t is the subgroup $\langle \omega^{d_t} \rangle$ of* *order* $\frac{m}{d_t}$, *where*

(6) $$d_t=(r^t-1,m)\,.$$

By this Lemma, all the one-dimensional representations of H_t are given by

(7) $$S^{(t)}_{\alpha,\beta}(\omega^\nu\sigma^{t\mu})=\exp\frac{2\pi i\alpha\nu}{d_t}\exp\frac{2\pi i\beta t\mu}{s}\,,\qquad \omega^\nu\sigma^{t\mu}\in H_t\,,$$

where $$1\leqslant\alpha\leqslant d_t\,,\quad 1\leqslant\beta\leqslant\frac{s}{t}\,.$$

The induced matrix representation of G of $S^{(t)}_{\alpha,\beta}$ is denoted by

(8) $$\operatorname*{Ind}_{H_t\uparrow G} S^{(t)}_{\alpha,\beta}\quad\text{or}\quad \operatorname{Ind} S^{(t)}_{\alpha,\beta}\,.$$

we quote two lemmas from Curtis-Reiner [4, § 45] to examine when Ind $S^{(t)}_{\alpha,\beta}$ is irreducible and when two induced irreducible representations Ind $S^{(t)}_{\alpha,\beta}$ and Ind $S^{(t)}_{\alpha',\beta'}$ are equivalent.

LEMMA 2. *Let H be a normal subgroup of a group G, and let T be an irreducible representation of H. Then the induced representation* $\operatorname*{Ind}_{H\uparrow G} T$ *is irreducible if and only if, for all $x\notin H$, the representations T and $T^{(x)}: h\to T(x^{-1}hx)$ of H are not equivalent.*

LEMMA 3. *Let $H\lhd G$, and let T_1 and T_2 be irreducible representations of H, such that the induced representations* Ind T_1 and Ind T_2 *are irreducible. Then* Ind T_1 *and* Ind T_2 *are inequivalent representations of G if and only if, for any $x\in G$, the representation $T_1^{(x)}$ of H: $T_1^{(x)}(h)=T_1(x^{-1}hx)$, and T_2 are inequivalent.*

For $t=1$, the subgroup H_t is G itself and Ind $S^{(1)}_{\alpha,\beta}=S^{(1)}_{\alpha,\beta}$ $(1\leqslant\alpha\leqslant d_1,\ 1\leqslant\beta\leqslant s)$ are the one-dimensional representations of G. So in the following, we assume that t is a divisor of u such that $t\neq1$.

PROPOSITION 1. Ind $S^{(t)}_{\alpha,\beta}$ *is irreducible if and only if*

(9) $$r^\mu\alpha\not\equiv\alpha\pmod{d_t}\,,\quad 1\leqslant\mu\leqslant t-1\,.$$

PROOF. For any element $x=\omega^\nu\sigma^\mu\in G$, we have

(10) $$x^{-1}\omega x=\sigma^{-\mu}\omega\sigma^\mu=\omega^{r^\mu}\,,$$

(11) $$x^{-1}\sigma^t x=\sigma^{-\mu}\omega^{-\nu}\sigma^t\omega^\nu\sigma^\mu=\omega^{-\nu r^\mu-t(r^t-1)}\sigma^t\,,\quad d_t\,|\,r^t-1\,.$$

By Lemma 2, (10), and (11), we have

Ind $S^{(t)}_{\alpha,\beta}$ is irreducible

$\Longleftrightarrow S^{(t)}_{\alpha,\beta}\neq(S^{(t)}_{\alpha,\beta})^{(x)}$ for all $x\notin H_t$,

$\Longleftrightarrow S^{(t)}_{\alpha,\beta}(\omega)\neq S^{(t)}_{\alpha,\beta}(x^{-1}\omega x)$ or $S^{(t)}_{\alpha,\beta}(\sigma^t)\neq S^{(t)}_{\alpha,\beta}(x^{-1}\sigma^t x)$ for all $x\notin H_t$,

$\Longleftrightarrow \exp \dfrac{2\pi i\alpha}{d_t} = S^{(t)}_{\alpha,\beta}(\omega) \neq S^{(t)}_{\alpha,\beta}(x^{-1}\omega x) = \exp \dfrac{2\pi i\alpha}{d_t} r^{\mu}$ for all $x = \omega^{\nu}\sigma^{\mu} \notin H_t$,

$\Longleftrightarrow r^{\mu}\alpha \not\equiv \alpha \pmod{d_t}, \quad 1 \leqslant \mu \leqslant t-1.$ q.e.d.

PROPOSITION 2. *Let* $\mathrm{Ind}\, S^{(t)}_{\alpha,\beta}$ *and* $\mathrm{Ind}\, S^{(t)}_{\alpha',\beta'}$ *be irreducible. Then* $\mathrm{Ind}\, S^{(t)}_{\alpha,\beta}$ *and* $\mathrm{Ind}\, S^{(t)}_{\alpha',\beta'}$ *are inequivalent if and only if*

$$\beta \neq \beta' \text{ or } \alpha r^{\mu} \not\equiv \alpha' \pmod{d_t}, \quad 1 \leqslant \mu \leqslant t. \tag{12}$$

PROOF. By Lemma 3, (10), and (11), we have

$\mathrm{Ind}\, S^{(t)}_{\alpha,\beta}$ and $\mathrm{Ind}\, S^{(t)}_{\alpha',\beta'}$ are inequivalent

$\Longleftrightarrow$ for every $x \in G$, $(S^{(t)}_{\alpha,\beta})^{(x)} \neq S^{(t)}_{\alpha',\beta'}$,

$\Longleftrightarrow$ for every $x \in G$, $S^{(t)}_{\alpha,\beta}(x^{-1}\omega x) \neq S^{(t)}_{\alpha',\beta'}(\omega)$ or $S^{(t)}_{\alpha,\beta}(x^{-1}\sigma^t x) \neq S^{(t)}_{\alpha',\beta'}(\sigma^t)$,

$\Longleftrightarrow \exp \dfrac{2\pi i\alpha}{d_t} r^{\mu} \neq \exp \dfrac{2\pi i\alpha'}{d_t}, \quad 1 \leqslant \mu \leqslant t$, or $\exp \dfrac{2\pi i\beta t}{s} \neq \exp \dfrac{2\pi i\beta' t}{s}$,

$\Longleftrightarrow \alpha r^{\mu} \not\equiv \alpha' \pmod{d_t}, \quad 1 \leqslant \mu \leqslant t$, or $\beta \neq \beta'$. q.e.d.

PROPOSITION 3. *Let t and t' be any divisors of u, such that $t \neq t'$. Then* $\mathrm{Ind}\, S^{(t)}_{\alpha,\beta}$ *and* $\mathrm{Ind}\, S^{(t')}_{\alpha',\beta'}$ *are not equivalent* $\left(1 \leqslant \alpha \leqslant d_t,\ 1 \leqslant \beta \leqslant \dfrac{s}{t},\ 1 \leqslant \alpha' \leqslant d_{t'},\ 1 \leqslant \beta' \leqslant \dfrac{s}{t'}\right)$.

PROOF. Since $[G:H_t]=t$, $[G:H_{t'}]=t'$, the degrees of the representations $\mathrm{Ind}\, S^{(t)}_{\alpha,\beta}$ and $\mathrm{Ind}\, S^{(t')}_{\alpha',\beta'}$ are t and t', respectively. So the assertion is obvious.

Let us set

$$N(t) = \#\{\alpha;\ 1 \leqslant \alpha \leqslant d_t,\ r^{\mu}\alpha \not\equiv \alpha \pmod{d_t},\ 1 \leqslant \mu < t\}.$$

Propositions 1 and 2 show that, for a fixed t, the number of inequivalent irreducible representations induced from H_t is

$$\frac{sN(t)}{t^2}. \tag{13}$$

For any α, $1 \leqslant \alpha \leqslant d_t$, there exists the smallest positive integer $\xi(\alpha)$ such that $r^{\xi(\alpha)}\alpha \equiv \alpha \pmod{d_t}$. By (6), $\xi(\alpha)$ divides t. Let

$$t = p_1^{b_1} p_2^{b_2} \cdots p_l^{b_l}$$

be the decomposition of t into prime factors. Put

$$\Gamma(t) = \{p_1^{b_1-\lambda_1} p_2^{b_2-\lambda_2} \cdots p_l^{b_l-\lambda_l};\ \lambda_i = 0, 1,\ 1 \leqslant i \leqslant l\}. \tag{14}$$

We define the degree of an element of $\Gamma(t)$ as follows:

$$\deg (p_1^{b_1-\lambda_1} p_2^{b_2-\lambda_2} \cdots p_l^{b_l-\lambda_l}) = (b_1-\lambda_1) + (b_2-\lambda_2) + \cdots + (b_l-\lambda_l). \tag{15}$$

For every $\alpha (1 \leqslant \alpha \leqslant d_t)$, consider the subset of $\Gamma(t)$ composed of the elements divided by $\xi(\alpha)$. In this subset there exists the unique element of smallest degree. We denote it by $\Xi(\alpha)$. Then Ξ is a mapping from the set $\{1, 2, \cdots, d_t\}$ to $\Gamma(t)$. For an element w of $\Gamma(t)$, put

(16) $$M_t(w)=\#\{\alpha ; 1\leq\alpha\leq d_t, \Xi(\alpha)=w\} .$$

It is easily verified that $N(t)=M_t(t)$. For $0\leq j\leq l$, define

(17) $$\Gamma_j(t)=\{w\in\Gamma(t) ; \deg(w)=(b_1-1)+\cdots+(b_l-1)+j\} .$$

LEMMA 4. *For* $w\in\Gamma_k(t)$, $0\leq k\leq l$,

$$M_t(w)=\sum_{j=0}^{k}(-1)^{k-j}\sum_{\substack{v\in\Gamma_j(t)\\ v|w}} d_v , \quad \textit{where } d_v=(r^v-1, m) .$$

In particular we have

(18) $$N(t)=M_t(t)=\sum_{j=0}^{l}(-1)^{l-j}\sum_{v\in\Gamma_j(t)} d_v .$$

PROOF. Since we fix a divisor t of u, we write $M=M_t$, $\Gamma_\nu=\Gamma_\nu(t)$, etc. Remark that if $v|v'|u$, then $(r^v-1, d_{v'})=d_v$. We see that

$$M(w)=d_w , \quad w\in\Gamma_0=\{p_1^{b_1-1}\cdots p_l^{b_l-1}\} .$$

In fact, $\Xi(\alpha)=w$, if and only if $(r^w-1)\alpha\equiv 0 \pmod{d_t}$. The number of such $\alpha (1\leq\alpha\leq d_t)$ is just d_w.

Assume that for any j and any v such that $0\leq j\leq k-1<l$, and $v\in\Gamma_j$, we have

$$M(v)=\sum_{\nu=0}^{j}(-1)^{j-\nu}\sum_{\substack{z\in\Gamma_\nu\\ z|v}} d_z .$$

Let $w\in\Gamma_k$. If $\Xi(\alpha)=w$, then

(19) $$(r^w-1)\alpha\equiv 0 , \quad \pmod{d_t} .$$

Conversely, when $\alpha \pmod{d_t}$ satisfies (19), then $\Xi(\alpha)$ divides w. Since the number of such α is d_w, we have

(20) $$M(w)=d_w-\{\sum_{\substack{v\in\Gamma_{k-1}\\ v|w}} M(v)+\sum_{\substack{v\in\Gamma_{k-2}\\ v|w}} M(v)+\cdots+\sum_{\substack{v\in\Gamma_0\\ v|w}} M(v)\} .$$

By the assumption of induction, the right side is written as a linear combination of d_v with integer coefficients, where v runs over the elements of Γ such that $v|w$. We compute the coefficient of d_v. As $w\in\Gamma_k$, we may assume without loss of generality that

$$w=p_1^{b_1}\cdots p_k^{b_k}p_{k+1}^{b_{k+1}-1}\cdots p_l^{b_l-1} .$$

Let $v\in\Gamma_j$ $(0\leq j\leq k-1)$ be a divisor of w. Then v is, for example, of the form:

$$v=p_1^{b_1}\cdots p_j^{b_j}p_{j+1}^{b_{j+1}-1}\cdots p_k^{b_k-1}\cdots p_l^{b_l-1} .$$

From these expressions we see easily that, for $0\leqq\nu\leqq k-1-j$, the coefficient of d_v in

$$\sum_{v'\in\Gamma_{j-\nu},v'|w} M(v')$$

is $(-1)^{\nu}\binom{k-j}{\nu}$, so that the coefficient of d_v in the right side of (20) is

$$-\sum_{\nu=0}^{k-j-1}(-1)^{\nu}\binom{k-j}{\nu}=(-1)^{k-j}\,.$$

Thus we have

$$M(w)=\sum_{j=0}^{k}(-1)^{k-j}\sum_{\substack{v\in\Gamma_j\\ v|w}} d_v\ ,$$

and the induction is completed.

Up to now we have assumed that $t\neq 1$. For $t=1$, put

$$\Gamma_0(1)=\{1\} \text{ and } N(1)=d_1\ .$$

PROPOSITION 4. *For a divisor t of u, let $t=p_1^{b_1}\cdots p_l^{b_l}$ be the decomposition of t into prime-factors. Then the number of inequivalent irreducible representations of G induced from the subgroup H_t is equal to*

$$\frac{s}{t^2}N(t)=\frac{s}{t^2}\left[\sum_{j=0}^{l}(-1)^{l-j}\sum_{v\in\Gamma_j(t)} d_v\right], \tag{21}$$

where $d_v=(r^v-1, m)$, and $\Gamma_j(t)$ is defined by (17).

Since $[G:H_t]=t$, the sum of squares of the degrees of the inequivalent irreducible representations induced from the subgroup H_t is equal to $s\cdot N(t)$. Therefore we shall compute the sum:

$$\tilde{N}=\sum_{1\leq t\leq u,t|u} N(t)\ . \tag{22}$$

By Lemma 4, $\tilde{N}$ is a $\boldsymbol{Z}$-linear combination of d_v, where v runs over the divisors of u. Let $u=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ $(\prod_{i=1}^{n}a_i\neq 0)$ be the decomposition into prime-factors. For any divisor $v=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ of u, put

$$k=\#\{i\,;\,1\leqq i\leqq n,\ e_i\neq a_i\}\ .$$

We may assume that v is of the form:

$$v=p_1^{e_1}\cdots p_k^{e_k}p_{k+1}^{a_{k+1}}\cdots p_n^{a_n}\,,\quad (0\leqq e_1<a_1,\cdots,0\leqq e_k<a_k)\ .$$

The d_v appears as a term in $N(t)$, if and only if $v|t$ and $f_i-1\leqq e_i\leqq f_i$ $(i=1,2,\cdots,k)$ where $t=p_1^{f_1}\cdots p_k^{f_k}p_{k+1}^{a_{k+1}}\cdots p_n^{a_n}$. In this case the coefficient of d_v in $N(t)$ is $(-1)^{\nu}$, where

$$\nu=\#\{i\,;\,1\leqq i\leqq k,\ f_i=e_i+1\}\ .$$

Hence for $v \neq u$, the coefficient of d_v in $\tilde{N}$ is equal to

$$\sum_{\nu=0}^{k} (-1)^{\nu} \binom{k}{\nu} = (1-1)^k = 0 .$$

Clearly, the coefficient of d_u in $\tilde{N}$ is equal to 1. Recall that $d_u = (r^u - 1, m) = m$. Therefore we have

$$\tilde{N} = \sum_{1 \leq t \leq u, t|u} N(t) = m ,$$

hence

$$s \cdot \tilde{N} = sm = \#(G) .$$

However $s\tilde{N}$ is the sum of squares of the degrees of the inequivalent irreducible representations among the $\operatorname{Ind}_{H_t \uparrow G} S^{(t)}_{\alpha,\beta}$, where t runs over all the divisors of u, and $1 \leq \alpha \leq d_t$, $1 \leq \beta \leq \frac{s}{t}$. Summarizing, we have

THEOREM 1.[*] *Let G be a non-abelian metacyclic group such that G is a semi-direct product $G = \langle\omega\rangle \cdot \langle\sigma\rangle$, where $\langle\omega\rangle$ is a cyclic normal subgroup of order m and $\langle\sigma\rangle$ is a cyclic group of order s. The notation being as before, any irreducible representation of G is equivalent to one of*

$$\operatorname{Ind}_{H_t \uparrow G} S^{(t)}_{\alpha,\beta} , \quad t|u, \ 1 \leq \alpha \leq d_t, \ 1 \leq \beta \leq \frac{s}{t} ,$$

where $S^{(t)}_{\alpha,\beta}$ is a linear character of the subgroup H_t of G, defined by (7). *The conditions of irreducibility and inequivalence of* $\operatorname{Ind} S^{(t)}_{\alpha,\beta}$ *and the number of such representations are given by Propositions* 1—4.

COROLLARY. *The notation being as in Theorem 1, suppose that $d_t = (r^t - 1, m) = 1$ for all $t|u$, $t \neq u$. Then every irreducible representation of G is either one-dimensional or equivalent to one of* $\operatorname{Ind} S^{(u)}_{\alpha,\beta}$, $1 \leq \alpha \leq m-1$, $1 \leq \beta \leq \frac{s}{u}$, *that are induced from the subgroup H_u. The number of distinct irreducible representations of G is equal to*

$$s + \frac{s(m-1)}{u^2} . \tag{23}$$

PROOF. From Lemma 4 and the fact $d_t = 1$ $(t \neq u)$, it is easily seen that

$$N(u) = d_u + \sum_{\nu=0}^{n-1} (-1)^{n-\nu} \binom{n}{\nu} = m - 1 ,$$

$$N(t) = \sum_{j=0}^{l} (-1)^{l-j} \binom{l}{j} = 0 , \quad t|u, \ 1 < t < u ,$$

$$N(1) = 1 ,$$

---

[*] Professor H. Nagao kindly adviced to the author that the first part of Theorem 1 can be deduced from results of Clifford [3].

where n and l are the numbers of primes dividing u and t, respectively. q.e.d.

EXAMPLE 1. Let G be a metacyclic group satisfying the relations

$$w^p=\sigma^s=1\ ,\quad \sigma^{-1}\omega\sigma=\omega^r\ ,\quad u=\text{order of } r(\text{mod } p)\ ,$$

where p is a rational odd prime. Then $d_t=(r^t-1, p)=1$ for all $t|u$, $t\neq u$. Hence every irreducible representation of G is either one of $S_{1,\beta}^{(1)}$, $1\leqslant\beta\leqslant s$ or one of $S_{\alpha,\beta}^{(u)}$, $1\leqslant\alpha\leqslant p-1$, $1\leqslant\beta\leqslant\frac{s}{u}$. The number of irreducible representations of G is equal to

$$s+\frac{s(p-1)}{u^2}\ .$$

EXAMPLE 2. (A Q-elementary group G at the prime p whose p-Sylow groups are cyclic). In this case, the defining relations are

$$\omega^m=\sigma^{p^a}=1\ ,\quad \sigma^{-1}\omega\sigma=\omega^r\ ,\quad p=\text{a rational prime.}$$

Since $u|p^a$, put $u=p^b$ and $t=p^c$ $(0<c\leqslant b)$. From Lemma 4, it follows that

$$N(p^c)=d_{p^c}-d_{p^{c-1}}\ ,\quad N(1)=d_1\ ,$$

so that the number of irreducible representations of G is equal to

$$p^a d_1+\sum_{c=1}^{b}\frac{p^a(d_{p^c}-d_{p^{c-1}})}{p^{2c}}\ .$$

3. The structure of group algebras $Q[G]$

The notation being as in § 2, we determine first the induced matrix representations $\operatorname{Ind} S_{\alpha,\beta}^{(t)}$. For the sake of brevity, put

$$U_{\alpha,\beta}^{(t)}=\operatorname*{Ind}_{H_t\uparrow G} S_{\alpha,\beta}^{(t)}\ . \tag{1}$$

A left coset decomposition of G by H_t is

$$G=H_t\cup\sigma H_t\cup\cdots\cup\sigma^{t-1}H_t\ .$$

Therefore we have

$$U_{\alpha,\beta}^{(t)}(\omega)=\begin{pmatrix}\zeta^\alpha & & & 0\\ & \zeta^{\alpha r} & & \\ & & \ddots & \\ 0 & & & \zeta^{\alpha r^{t-1}}\end{pmatrix},\qquad \zeta=\exp\frac{2\pi i}{d_t}\ , \tag{2}$$

$$U_{\alpha,\beta}^{(t)}(\sigma)=\begin{pmatrix}0 & \cdots\cdots & 0 & \xi^\beta\\ 1 & & & 0\\ & \ddots & & \vdots\\ 0 & & 1 & 0\end{pmatrix},\qquad \xi=\exp\frac{2\pi i t}{s}\ , \tag{3}$$

$$U_{\alpha,\beta}^{(t)}(\sigma^t)=\xi^\beta\cdot 1_t\ , \tag{4}$$

where 1_t is the identity element of the complete matric algebra $M_t(\boldsymbol{C})$. Denote by $\chi_{\alpha,\beta}^{(t)}$ the character of the representation $U_{\alpha,\beta}^{(t)}$. Since H_t is a normal subgroup of G,

$$(5)\qquad \chi_{\alpha,\beta}^{(t)}(\omega^\nu\sigma^\mu)=0 \text{ for all } \omega^\nu\sigma^\mu\notin H_t, \text{ i.e., for } \mu\not\equiv 0 \pmod t.$$

Because of

$$(6)\qquad U_{\alpha,\beta}^{(t)}(\omega^\nu\sigma^{t\mu})=\xi^{\beta\mu}\begin{pmatrix}\zeta^{\alpha\nu} & & & 0\\ & \zeta^{\alpha r\nu} & & \\ & & \ddots & \\ 0 & & & \zeta^{\alpha r^{t-1}\nu}\end{pmatrix},$$

we have

$$(7)\qquad \chi_{\alpha,\beta}^{(t)}(\omega^\nu\sigma^{t\mu})=\xi^{\beta\mu}(\zeta^{\alpha\nu}+\zeta^{\alpha r\nu}+\cdots+\zeta^{\alpha r^{t-1}\nu}),\quad 1\leqq\nu\leqq m,\ 1\leqq\mu\leqq\frac{s}{t}.$$

Therefore the character field of $\chi_{\alpha,\beta}^{(t)}$ is:

$$(8)\qquad \boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})=\boldsymbol{Q}(\xi^\beta, \eta_1, \eta_2, \cdots, \eta_m),$$

where $\qquad \eta_\nu=\zeta^{\alpha\nu}+\zeta^{\alpha r\nu}+\cdots+\zeta^{\alpha r^{t-1}\nu},\quad 1\leqq\nu\leqq m.$

From now on, we assume that $(m, s)=1$ and that the induced representation $U_{\alpha,\beta}^{(t)}$ is irreducible. Under these assumptions, $\boldsymbol{Q}(\zeta)\cap\boldsymbol{Q}(\xi)=\boldsymbol{Q}$, and $\zeta^\alpha, \zeta^{\alpha r}, \cdots, \zeta^{\alpha r^{t-1}}$ are distinct conjugates over $\boldsymbol{Q}$.

LEMMA 5. *The field $\boldsymbol{Q}(\xi^\beta, \zeta^\alpha)$ is a cyclic extension of degree t over the character field $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$, the Galois group of which is generated by τ:*

$$(9)\qquad \tau(\xi^\beta)=\xi^\beta,\quad \tau(\zeta^\alpha)=\zeta^{\alpha r}.$$

PROOF. In the Galois group of $\boldsymbol{Q}(\xi^\beta, \zeta^\alpha)$ over $\boldsymbol{Q}(\xi^\beta)$, τ generates a cyclic subgroup $\langle\tau\rangle$ of order t. Let k be the corresponding field to $\langle\tau\rangle$ in the sense of Galois theory. On account of

$$\tau(\eta_\nu)=\zeta^{\alpha r\nu}+\zeta^{\alpha r^2\nu}+\cdots+\zeta^{\alpha r^{t-1}\nu}+\zeta^{\alpha\nu}=\eta_\nu,\quad 1\leqq\nu\leqq m,$$

$\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})=\boldsymbol{Q}(\xi^\beta, \eta_1, \cdots, \eta_m)$ is contained in the field k. We show that $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})=k$. In fact, put

$$F(x)=(x-\zeta^\alpha)(x-\zeta^{\alpha r})\cdots(x-\zeta^{\alpha r^{t-1}})=x^t+a_1x^{t-1}+\cdots+a_t.$$

Then it is easily verified that

$$\{a_1, a_2, \cdots, a_t\}\subset\boldsymbol{Q}(\eta_1, \eta_2, \cdots, \eta_t).$$

So that ζ^α is a root of the polynomial $F(x)$ whose coefficients are in $\boldsymbol{Q}(\eta_1, \eta_2, \cdots, \eta_t)$. Therefore we have

$$[\boldsymbol{Q}(\xi^\beta, \zeta^\alpha) : \boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})] \leqq [\boldsymbol{Q}(\zeta^\alpha) : \boldsymbol{Q}(\eta_1, \cdots, \eta_t)] \leqq t\ .$$

Since $[\boldsymbol{Q}(\xi^\beta, \zeta^\alpha) : k] = t$ and $k \supset \boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$, we conclude that $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)}) = k$, as required.

REMARK. From the proof we have $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)}) = \boldsymbol{Q}(\xi^\beta, \eta_1, \cdots, \eta_t)$.

Until the end of this section we fix the irreducible representation $U_{\alpha,\beta}^{(t)}$ and write briefly as $U = U_{\alpha,\beta}^{(t)}$, $\chi = \chi_{\alpha,\beta}^{(t)}$.

LEMMA 6. *Let $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ be the matrix algebra generated by $U(\sigma^t)$ and $U(\omega)$ with rational coefficients. Then there is an isomorphism*

$$\Phi : \boldsymbol{Q}(\xi^\beta, \zeta^\alpha) \simeq \boldsymbol{Q}(U(\sigma^t), U(\omega)) \tag{10}$$

such that

$$\Phi(\xi^\beta) = U(\sigma^t) \text{ and } \Phi(\zeta^\alpha) = U(\omega)\ . \tag{11}$$

PROOF. On account of the fact

$$U(\omega) = \begin{pmatrix} \zeta^\alpha & & & 0 \\ & \zeta^{\alpha r} & & \\ & & \ddots & \\ 0 & & & \zeta^{\alpha r^{t-1}} \end{pmatrix}, \qquad U(\sigma^t) = \xi^\beta \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},$$

any element Θ of $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ is of the form:

$$\Theta = \begin{pmatrix} F(\zeta^\alpha) & & & 0 \\ & F(\zeta^{\alpha r}) & & \\ & & \ddots & \\ 0 & & & F(\zeta^{\alpha r^{t-1}}) \end{pmatrix},$$

where $F(x)$ is a polynomial in $\boldsymbol{Q}(\xi^\beta)[x]$. Since $\zeta^\alpha, \zeta^{\alpha r}, \cdots, \zeta^{\alpha r^{t-1}}$ are distinct conjugates over $\boldsymbol{Q}(\xi^\beta)$, $F(\zeta^\alpha), F(\zeta^{\alpha r}), \cdots, F(\zeta^{\alpha r^{t-1}})$ are conjugates over $\boldsymbol{Q}(\xi^\beta)$. So that $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ is a field. The latter half of this Lemma is immediate from the above proof.

By means of the isomorphism Φ, the field $\boldsymbol{Q}(\chi)$ is mapped onto $\boldsymbol{Q}(\chi)\cdot 1_t$. Let us define an endomorphism $\tilde{\tau}$ of $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ by

$$\tilde{\tau} :\ \Theta \to U(\sigma)^{-1}\Theta U(\sigma)\ ,\quad \Theta \in \boldsymbol{Q}(U(\sigma^t)\ ,\ U(\omega))\ . \tag{12}$$

Then we have

$$\tilde{\tau} :\ U(\sigma^t) \to U(\sigma^t)\ , \tag{13}$$

$$\tilde{\tau} :\ U(\omega) \to U(\sigma)^{-1} U(\omega) U(\sigma) = U(\omega)^r\ . \tag{14}$$

$\tilde{\tau}$ is precisely the automorphism of $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ that corresponds to the automorphism τ of $\boldsymbol{Q}(\xi^\beta, \zeta^\alpha)$.

LEMMA 7. *$1_t, U(\sigma), \cdots, U(\sigma)^{t-1}$ are linearly independent over the field $\boldsymbol{Q}(U(\sigma^t), U(\omega))$.*

PROOF. Owing to (3), we have

$$U(\sigma)^{\mu}=\left(\begin{array}{ccc|ccc} & & & \xi^{\beta} & & 0 \\ & 0 & & & \ddots & \\ & & & 0 & & \xi^{\beta} \\ \hline 1 & & 0 & & & \\ & \ddots & & & 0 & \\ 0 & & 1 & & & \end{array}\right) \begin{array}{l} \uparrow \\ \mu \\ \downarrow \\ \uparrow \\ t-\mu \\ \downarrow \end{array} \qquad 0 \leqq \mu \leqq t-1 .$$

On the other hand, any element of $\boldsymbol{Q}(U(\sigma^t), U(\omega))$ is a diagonal matrix. Therefore the assertion is obvious.

The enveloping algebra $\mathrm{env}_Q(U)$ over $\boldsymbol{Q}$ of the irreducible representation $U=U_{\alpha,\beta}^{(t)}$ is the matrix algebra $\boldsymbol{Q}(U(\omega), U(\sigma))$. From Lemma 7, it follows that

$$\mathrm{env}_Q(U)=\sum_{\mu=0}^{t-1} U(\sigma)^{\mu}\cdot \boldsymbol{Q}(U(\sigma^t), U(\omega)) \quad \text{(direct sum)}. \tag{15}$$

Thus we have obtained

THEOREM 2. *Let G be a metacyclic group containing a cyclic normal subgroup of order m and with a cyclic factor group G/H of order s such that $(m, s)=1$. The notation being as in Theorem 1, the enveloping algebra over $\boldsymbol{Q}$ of any irreducible representation $U_{\alpha,\beta}^{(t)}=\operatorname{Ind}_{H_t \uparrow G} S_{\alpha,\beta}^{(t)}$ of G is isomorphic to the cyclic algebra with center $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$:*

$$\mathrm{env}_Q(U_{\alpha,\beta}^{(t)}) \simeq (\xi^{\beta}, \boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha}), \tau)_{Q(\chi_{\alpha,\beta}^{(t)})} \tag{16}$$

where $\zeta=\exp\dfrac{2\pi i}{d_t}$, $\xi=\exp\dfrac{2\pi i t}{s}$, and τ is a generating automorphism of $\boldsymbol{Q}(\zeta^{\alpha}, \xi^{\beta})$ over the character field $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$. (For $t=1$, the right side of (16) indicates the field $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(1)})=\boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha})$).

THEOREM 2′. *The assumption and the notation being as in Theorem 2, we have*

$$\boldsymbol{Q}[G] \simeq \sum_{\chi_{\alpha,\beta}^{(t)}} (\xi^{\beta}, \boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha}), \tau)_{Q(\chi_{\alpha,\beta}^{(t)})} \qquad \textit{(direct sum)} \tag{17}$$

where the sum ranges over distinct, irreducible, and not algebraically conjugate characters $\chi_{\alpha,\beta}^{(t)}$.

REMARK: Let $\chi_{\alpha_1,\beta_1}^{(t)}$ and $\chi_{\alpha_2,\beta_2}^{(t)}$ be distinct irreducible characters. Then they are algebraically conjugate if and only if $d_{t,\alpha_1}=d_{t,\alpha_2}$ and $v_{t,\beta_1}=v_{t,\beta_2}$, where $d_{t,\alpha_i}=\dfrac{d_t}{(d_t, \alpha_i)}$ and $v_{t,\beta_i}=\dfrac{s/t}{(s/t, \beta_i)}$, $i=1, 2$.

4. The Schur index

At first we recall parts of the theory of cyclic algebras and the class field theory. Let K be a cyclic extension of degree n over an algebraic number field k, the Galois group of which is generated by τ, and let a be an element of $k^{\times}$. If $\frac{\nu_{\mathfrak{p}}}{n}$ (mod^{+} 1) is the local invariant of the cyclic algebra (a, K, τ) at a prime spot $\mathfrak{p}$ of k, the (global) norm residue symbol is

(1) $$\left(\frac{a, K/k}{\mathfrak{p}}\right)=\tau^{-\nu_{\mathfrak{p}}} .$$

Let $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ represent the isomorphy type of the completion of K/k for $\mathfrak{P}|\mathfrak{p}$. By the local class field theory the local norm residue symbol $(\gamma, K_{\mathfrak{P}}/k_{\mathfrak{p}})$, where $\gamma\in k_{\mathfrak{p}}^{\times}$, gives a canonical isomorphism of the norm residue group $k_{\mathfrak{p}}^{\times}/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})$ onto $\mathfrak{G}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$. The decomposition group of K/k for the $\mathfrak{P}|\mathfrak{p}$ is just $\mathfrak{G}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$, and

(2) $$\left(\frac{a, K/k}{\mathfrak{p}}\right)=(a, K_{\mathfrak{P}}/k_{\mathfrak{p}}) \quad \text{for } a\in k^{\times} .$$

Therefore the local index of (a, K, τ) at $\mathfrak{p}$ is the order of $(a, K_{\mathfrak{P}}/k_{\mathfrak{p}})=\left(\frac{a, K/k}{\mathfrak{p}}\right)$ in the Galois group $\mathfrak{G}(K/k)$. The (global) index of (a, K, τ) is the least common multiple of all the local indices.

From now on, the assumption and the notation are the same as in Theorem 2. The Schur index of the irreducible representation $U_{\alpha,\beta}^{(t)}$ of G is the index of the algebra $\mathrm{env}_{\boldsymbol{Q}}(U_{\alpha,\beta}^{(t)})$, which is by Theorem 2, isomorphic to the cyclic algebra $(\xi^{\beta}, \boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha}), \tau)$ with center $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$. Hence we calculate with the norm residue symbols

(3) $$\left(\frac{\xi^{\beta}, \boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha})/\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})}{\mathfrak{p}}\right)$$

for all prime spots $\mathfrak{p}$ of $\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)})$. For the sake of brevity, put

(4) $$K=\boldsymbol{Q}(\xi^{\beta}, \zeta^{\alpha}) \text{ and } k=\boldsymbol{Q}(\chi_{\alpha,\beta}^{(t)}) .$$

Let p be a rational prime, and let $\mathfrak{p}$ and $\mathfrak{P}$ be prime ideals of k and K respectively, that divide p. Let $e=e_{\mathfrak{p}}$ be the ramification exponent of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ and Π be a prime element of $K_{\mathfrak{P}}$. Put $\psi=N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\Pi)$, $N_{k/\boldsymbol{Q}}(\mathfrak{p})=q$, and $N_{K/\boldsymbol{Q}}(\mathfrak{P})=q^{h}$, where q is a power of p. If $\tilde{\theta}\in K_{\mathfrak{P}}$ is a primitive $(q^{h}-1)$-th root of unity, $\tilde{\theta}\tilde{\theta}^{q}\cdots\tilde{\theta}^{q^{h-1}}=\theta$ is a primitive $(q-1)$-th root of unity of $k_{\mathfrak{p}}$, and $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\tilde{\theta})=\theta^{e}$. It is well known that every element $a\in K_{\mathfrak{P}}^{\times}$ has a unique representation

$$a=\Pi^{n}\tilde{\theta}^{l}\gamma , \quad n\in \boldsymbol{Z} , \quad l \bmod q^{h}-1 , \quad \gamma\text{: Einseinheit} .$$

(Cf. Hasse [7]). Therefore we have

$$N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})=\{\phi^n\theta^l N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\gamma)\,;\ n\in \boldsymbol{Z},\ 1\leq l\leq q^h-1,\ \gamma:\text{Einseinheit of } K_{\mathfrak{P}}\}\ .$$

Recall that $\boldsymbol{Q}\left(\exp\frac{2\pi it\beta}{s}\right)\subset k\subset K=\boldsymbol{Q}\left(\exp\frac{2\pi it\beta}{s},\ \exp\frac{2\pi i\alpha}{d_t}\right)$, and K/k is a cyclic extension of degree t, and $t|s$, $d_t|m$, $(s,m)=1$, so that $(t,d_t)=1$. If $\mathfrak{p}$ does not divide d_t, then $\mathfrak{p}$ is not ramified in $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, so that $\left(\frac{\xi^\beta,\ K/k}{\mathfrak{p}}\right)=(\xi^\beta,\ K_{\mathfrak{P}}/k_{\mathfrak{p}})=1$, because ξ^β is a unit of $k_{\mathfrak{p}}$. If $\mathfrak{p}$ divides d_t, then $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is a tamely ramified cyclic extension. Therefore its ramification exponent $e=e_{\mathfrak{p}}(\geq 1)$ divides $q-1$ (Hasse [7, p. 187]). Thus we have

$$N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})=\left\{\phi^n\theta^{e\lambda}N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\gamma)\,;\ n\in\boldsymbol{Z},\ 1\leq\lambda\leq\frac{q-1}{e},\ \gamma:\text{Einseinheit of } K_{\mathfrak{P}}\right\}\ .$$

Let us set

$$v_{t,\beta}=\frac{s/t}{(s/t,\ \beta)}\ . \tag{5}$$

Since $\xi^\beta\in k_{\mathfrak{p}}$ is a primitive $v_{t,\beta}$-th root of unity and $\mathfrak{p}$ does not divide $v=v_{t,\beta}$, we can assume that $\xi^\beta=\theta^{\frac{q-1}{v}}$, where $q=N_{k_{\mathfrak{p}}/\boldsymbol{Q}_p}(\mathfrak{p})$. If $\xi^{\beta x}\in N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})$ for some positive integer x, then $\xi^{\beta x}=\theta^{\frac{q-1}{v}x}=\phi^n\theta^{e\lambda}N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\gamma)$ for some n, λ, and γ. As $\xi^{\beta x}$ is a unit and $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\gamma)$ is an Einseinheit of $k_{\mathfrak{p}}$, it follows that $\theta^{\frac{q-1}{v}x}=\theta^{e\lambda}$, so that $e=e_{\mathfrak{p}}$ divides $\frac{q-1}{v_{t,\beta}}x$. Therefore the smallest positive integer x such that $\xi^{\beta x}\in N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})$ is $e_{\mathfrak{p}}/\left(e_{\mathfrak{p}},\ \frac{q-1}{v_{t,\beta}}\right)$. As the the map $\gamma\to(\gamma,\ K_{\mathfrak{P}}/k_{\mathfrak{p}})$, $\gamma\in k_{\mathfrak{p}}^{\times}$ gives an isomorphism of $k_{\mathfrak{p}}^{\times}/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^{\times})$ onto $\mathfrak{G}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$, the order of the norm residue symbol $\left(\frac{\xi^\beta,\ K/k}{\mathfrak{p}}\right)=(\xi^\beta,\ K_{\mathfrak{P}}/k_{\mathfrak{p}})$ is equal to

$$\frac{e_{\mathfrak{p}}}{\left(e_{\mathfrak{p}},\ \frac{q-1}{v_{t,\beta}}\right)}\ . \tag{6}$$

We compute the ramification exponent $e_{\mathfrak{p}}$ of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Let us set

$$d_{t,\alpha}=d_t/(d_t,\ \alpha)\ . \tag{7}$$

Then ζ^α is a primitive $d_{t,\alpha}$-th root of unity. Put $d_{t,\alpha}=p^a n$, where $\mathfrak{p}|p$ and $(p,n)=1$. For convenience, write $v=v_{t,\beta}$. The Galois group $\mathfrak{G}(K/\boldsymbol{Q})$ is isomorphic to $(\boldsymbol{Z} \bmod p^a nv)^{\times}$, which is further isomorphic to the direct product $\mathfrak{G}'$ of $(\boldsymbol{Z} \bmod p^a)^{\times}$, $(\boldsymbol{Z} \bmod n)^{\times}$, and $(\boldsymbol{Z} \bmod v)^{\times}$:

$$\mathfrak{G}'=\{(x,\ y,\ z)\,;\ x\in(\boldsymbol{Z}\ \mathrm{mon}\ p^a)^{\times},\ y\in(\boldsymbol{Z} \bmod n)^{\times},\ z\in(\boldsymbol{Z} \bmod v)^{\times}\}\ . \tag{8}$$

The operation in $\mathfrak{G}'$ and the isomorphism of $\mathfrak{G}(K/\boldsymbol{Q})$ onto $\mathfrak{G}'$ are as usual. In the following we identify $\mathfrak{G}(K/\boldsymbol{Q})$ with $\mathfrak{G}'$. It is clear that $\mathfrak{G}(K/Q)\ni\tau:\zeta^a\to\zeta^{ar}$, corresponds to $(r, r, 1)\in\mathfrak{G}'$, so that we have $\mathfrak{G}(K/k)=\{(r^\nu, r^\nu, 1); 0\leqslant\nu\leqslant t-1\}$. The inertia group of $\mathfrak{p}\subset k$, $\mathfrak{p}|p$ in $\mathfrak{G}(K/k)$ is

$$\mathfrak{G}(K/k)\cap\mathfrak{G}\left(K/\boldsymbol{Q}\left(\exp\frac{2\pi i}{v}, \exp\frac{2\pi i}{n}\right)\right),$$

where

$$\mathfrak{G}\left(K/\boldsymbol{Q}\left(\exp\frac{2\pi i}{v}, \exp\frac{2\pi i}{n}\right)\right)=\{(x, 1, 1); x\in(\boldsymbol{Z} \bmod p^a)^\times\}.$$

If t_n is the order of $r \pmod n$, it follows that the inertia group is $\left\{(r^{t_n\nu}, 1, 1); 0\leqslant\nu\leqslant\frac{t}{t_n}-1\right\}$, so that the ramification exponent $e_\mathfrak{p}$ is equal to $\frac{t}{t_n}$.

Next we calculate with the absolute norm $q=N_{k/Q}(\mathfrak{p})$ of $\mathfrak{p}$. The decomposition group of $\mathfrak{p}$ in $\mathfrak{G}(K/k)$ is

$$\{(r^\nu, r^\nu, 1); 0\leqslant\nu\leqslant t-1\}\cap\{(x, p^\lambda, p^\lambda); x\in(Z \bmod p^a)^\times, 0\leqslant\lambda\leqslant\bar{f}-1\},$$

where $\bar{f}$ is the order of $p \pmod{nv}$. Denote by f' the order of $p \pmod v$, and set

$$f=\#[\langle p^{f'} \pmod n\rangle\cap\langle r \pmod n\rangle]. \tag{9}$$

Then it is easily seen that the decomposition group of $\mathfrak{p}$ is of order $f\frac{t}{t_n}$. Consequently the relative degree of $\mathfrak{p}$ in K/k is equal to f and the absolute norm q of $\mathfrak{p}$ is

$$q=N_{k/Q}(\mathfrak{p})=p^{\bar{f}/f}. \tag{10}$$

Now we consider infinite prime spots $\mathfrak{p}_\infty$ of k.

(Case I) $\xi^\beta\neq\pm1$.

Then k is a totally imaginary number field, so that for every $\mathfrak{p}_\infty$, the local index at $\mathfrak{p}_\infty$ of the cyclic algebra $(\xi^\beta, K, \tau)_k$ is equal to 1.

(Case II) $\xi^\beta=1$.

Clearly for every $\mathfrak{p}_\infty$, the local index at $\mathfrak{p}_\infty$ of $(1, K, \tau)_k$ is equal to 1.

(Case III) $\xi^\beta=-1$ and k is imaginary.

This case is obvious.

(Case IV) $\xi^\beta=-1$ and k is real.

Since $N_{C/R}(\gamma)$, $\gamma\in\boldsymbol{C}^\times$ are positive real numbers, the local index at any $\mathfrak{p}_\infty$ of $(-1, K, \tau)_k$, $K=\boldsymbol{Q}(\zeta^a)$ is equal to 2. The condition $\xi^\beta=-1$ amounts to $2\beta=s/t$. k is real if and only if k is contained in $\boldsymbol{Q}(\zeta^a+\zeta^{-a})$. Recall that ζ^a is a primitive $d_{t,a}$-th root of unity. Therefore, k is real if and only if $2|t$ and $r^{t/2}\equiv-1$

$(\mathrm{mod}\, d_{t,\alpha})$. For any finite prime $\mathfrak{p}$ of k, the local index at $\mathfrak{p}$ of $(-1, K, \tau)_k$ is 1 or 2, so that in (Case IV), the (global) index of $(-1, K, \tau)_k$ is equal to 2.

We summarize the results that have been obtained.

THEOREM 3. *The assumption and the notation being the same as in Theorem 2, denote by* $\Lambda_{\mathfrak{p}}$, *the local index at* $\mathfrak{p}$ *of* $\mathrm{env}_Q(U_{\alpha,\beta}^{(t)})$, *where* $\mathfrak{p}$ *is a prime spot of* $Q(\chi_{\alpha,\beta}^{(t)})$. *Put*

$$d_{t,\alpha}=\frac{d_t}{(d_t, \alpha)}\,, \quad v_{t,\beta}=\frac{s/t}{(s/t, \beta)}\,.$$

(I) *If* $\mathfrak{p}$ *is a prime ideal such that* $\mathfrak{p}\nmid d_{t,\alpha}$, *then*

$$\Lambda_{\mathfrak{p}}=1\,.$$

(II) *If* $\mathfrak{p}$ *is a prime ideal such that* $\mathfrak{p}|p$, $d_{t,\alpha}=p^a n$, $(p, n)=1$, *then*

$$\Lambda_{\mathfrak{p}}=\frac{e_{\mathfrak{p}}}{\left(e_{\mathfrak{p}}, \dfrac{q-1}{v_{t,\beta}}\right)}\,, \quad e_{\mathfrak{p}}=\frac{t}{t_n}\,, \quad q=p^{\tilde{f}/f}\,,$$

where t_n *is the order of* r $(\mathrm{mod}\, n)$, $\tilde{f}$ *is the order of* p $(\mathrm{mod}\, nv_{t,\beta})$, *and*

$$f=\#[\langle p^{f'} (\mathrm{mod}\, n)\rangle \cap \langle r\ (\mathrm{mod}\, n)\rangle]\,,$$

f' *being the order of* p $(\mathrm{mod}\, v_{t,\beta})$.

(III) *For all infinite prime spots* $\mathfrak{p}_\infty$ *of* $Q(\chi_{\alpha,\beta}^{(t)})$,

$$\Lambda_{\mathfrak{p}_\infty}=1\,,$$

except the case that $s/t=2\beta$, $2|t$, *and* $r^{t/2}\equiv -1\ (\mathrm{mod}\, d_{t,\alpha})$. *In this case, for all* $\mathfrak{p}_\infty$

$$\Lambda_{\mathfrak{p}_\infty}=2\,.$$

THEOREM 4. *The assumption and the notation being as in Theorem 3, the Schur index of the irreducible representation* $U_{\alpha,\beta}^{(t)}$ *is the L.C.M. of*

$$\frac{\dfrac{t}{t_n}}{\left(\dfrac{t}{t_n}, \dfrac{p^{\tilde{f}/f}-1}{v_{t,\beta}}\right)}\,,$$

where p *runs over the primes dividing* $d_{t,\alpha}$, *except possibly the case where* $s/t=2\beta$, $2|t$, *and* $r^{t/2}\equiv -1\ (\mathrm{mod}\, d_{t,\alpha})$ *are satisfied. In this exceptional case, the Schur index of* $U_{\alpha,\beta}^{(t)}$ *is* 2.

COROLLARY. *The assumption and the notation being the same as in Theorem 3, let* $m=p^a$, *where* p *is a rational prime. Then the Schur index of any irreducible representation* $U_{\alpha,\beta}^{(t)}$ *of* G *is equal to*

$$\frac{t}{\left(t, \frac{p^f-1}{v_{t,\beta}}\right)},$$

where f is the order of $p \pmod{v_{t,\beta}}$, except the case satisfying the relations: $s/t=2\beta$, $2|t$, $r^{t/2}\equiv -1 \pmod{d_{t,\alpha}}$, and $t \mid \frac{p-1}{2}$. In this case the Schur index of $U^{(t)}_{\alpha,\beta}$ is equal to 2.

PROOF. We only remark that if $s/t=2\beta$, then $v_{t,\beta}=2$, $f=1$ so that

$$\frac{t}{\left(t, \frac{p^f-1}{v_{t,\beta}}\right)} = \begin{cases} 1 & t \mid \frac{p-1}{2}, \\ 2 & t \nmid \frac{p-1}{2}. \end{cases}$$

REMARK. Let G be a group satisfying

$$\omega^5=\sigma^8=1, \quad \sigma^{-1}\omega\sigma=\omega^{-1}.$$

Then the irreducible representation $U^{(2)}_{1,2}$ of G gives an example of the exceptional case.

EXAMPLE. (A $\boldsymbol{Q}$-elementary group at 2). The defining relations are

$$\omega^{15}=1, \quad \sigma^{-1}\omega\sigma=\omega^7, \quad \sigma^{16}=1, \quad \text{order of } 7 \pmod{15}=4.$$

From Theorem 1, we obtain easily the following results: The linear characters are

$$\chi^{(1)}_{\alpha,\beta}, \quad 1\leqslant\alpha\leqslant 3, \quad 1\leqslant\beta\leqslant 16.$$

The distinct induced characters are all of degree 4 and given by

$$\chi^{(4)}_{\alpha,\beta}, \quad 1\leqslant\alpha\leqslant 3, \quad 1\leqslant\beta\leqslant 4.$$

Among these

$$\chi^{(4)}_{1,1}, \quad \chi^{(4)}_{1,2}, \quad \chi^{(4)}_{1,4}, \quad \chi^{(4)}_{3,1}, \quad \chi^{(4)}_{3,2}, \quad \chi^{(4)}_{3,4}$$

are the characters that are not algebraically conjugate. By Theorem 4, we calculate readily their Schur indices:

	$\chi^{(4)}_{1,1}$	$\chi^{(4)}_{1,2}$	$\chi^{(4)}_{1,4}$	$\chi^{(4)}_{3,1}$	$\chi^{(4)}_{3,2}$	$\chi^{(4)}_{3,4}$
Schur index	2	1	1	4	2	1

In Appendix other examples are dealt with.

Appendix

Let p be a prime number, and consider the Davenport-Hasse curves C_n defined by the equations

$$(1)\qquad y^p - y = x^n\,,\quad (p, n) = 1\,,\quad n > 1\,,$$

over the prime field $GF(p)$. If we denote by θ a primitive $n(p-1)$-th root of unity in the algebraic closure of $GF(p)$, the map

$$(2)\qquad \sigma:\ (x, y) \to (\theta x, \theta^n y)$$

defines an automorphism of C_n of order $n(p-1)$. Since θ is a primitive $n(p-1)$-th root of unity, $\theta^n = r$ is a generator of the multiplicative group $GF(p)^\times$ and can be regarded as a rational integer. Clearly the curve C_n has another automorphism ω of order p:

$$(3)\qquad \omega:\ (x, y) \to (x, y+1)\,.$$

For automorphisms ρ_1, ρ_2 of C_n, the product $\rho_1\rho_2$ is defined by $(\rho_1\rho_2)(P) = \rho_2(\rho_1(P))$, $P \in C_n$. Then the following relations are easily verified:

$$(4)\qquad \omega^p = \sigma^{n(p-1)} = 1\,,\quad \sigma^{-1}\omega\sigma = \omega^r\,.$$

Hence ω and σ generate a metacyclic group G. We assume that $p \neq 2$, because in the case of $p=2$, G is abelian. As $(p, n(p-1)) = 1$, G is one of metacyclic groups that have been investigated, so that our results are applied to G.

According to Theorem 1, the irreducible and distinct representations of G are given by

$$\psi_\alpha,\ \alpha = 1, 2, \cdots, n(p-1)\,,\quad S_\beta,\ \beta = 1, 2, \cdots, n\,,$$

such that

$$\psi_\alpha(\omega^\nu\sigma^\mu) = \exp\frac{2\pi i\alpha\mu}{n(p-1)}\,,\quad \omega^\nu\sigma^\mu \in G\,,$$

$$S_\beta(\omega) = \begin{pmatrix} \zeta & & & 0 \\ & \zeta^r & & \\ & & \ddots & \\ 0 & & & \zeta^{r^{p-2}} \end{pmatrix},\quad \zeta = e^{\frac{2\pi i}{p}}\,,\qquad S_\beta(\sigma) = \begin{pmatrix} 0 & \cdots & 0 & \xi^\beta \\ 1 & & & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{pmatrix},\quad \xi = e^{\frac{2\pi i}{n}}\,.$$

The character χ_β of S_β is as follows:

$$\chi_\beta(\omega^\nu\sigma^\mu) = \begin{cases} 0\,, & \mu \not\equiv 0 \pmod{p-1}\,, \\ (p-1)\exp\dfrac{2\pi i\beta\mu}{n(p-1)}\,, & \mu \equiv 0 \pmod{p-1}\,,\quad \nu = 0\,, \\ -\exp\dfrac{2\pi i\beta\mu}{n(p-1)}\,, & \mu \equiv 0 \pmod{p-1}\,,\quad 1 \leqslant \nu \leqslant p-1\,. \end{cases}$$

By Theorem 4, Corollary, the Schur index of S_β is equal to

$$(5)\qquad \frac{p-1}{\left(p-1,\ \dfrac{p^f-1}{v_\beta}\right)},$$

where $v_\beta=\dfrac{n}{(n,\beta)}$, f=order of $p(\mathrm{mod}\ v_\beta)$.

We will determine the l-adic representation of the automorphism group G, where l is a prime number distinct from p. We give an outline of the proof. Let k be the algebraic closure of $GF(p)$, and put $w=x^{n(p-1)}$. Then the algebraic function field $k(x, y)$ defined by the equation (1) is a normal extension of $k(w)$, whose Galois group is precisely G. Denote by $\mathfrak{p}_0$ and $\mathfrak{p}_\infty$ the prime divisors of $k(w)$ that are the numerator and the denominator of the principal divisor (w), respectively. We can prove that in $k(x, y)/k(w)$, every prime divisor other than $\mathfrak{p}_0$ and $\mathfrak{p}_\infty$ is not ramified, and

$$\mathfrak{p}_0=(\mathfrak{P}_0\mathfrak{P}_1\cdots\mathfrak{P}_{p-1})^{n(p-1)},\quad \mathfrak{p}_\infty=\mathfrak{P}_\infty^{np(p-1)}.$$

The decomposition group of $\mathfrak{P}_\nu$ is $\omega^{-\nu}\langle\sigma\rangle\omega^\nu$. The divisors $\mathfrak{P}_\nu(0\leqq\nu\leqq p-1)$ and $\mathfrak{P}_\infty$ correspond respectively to the points $P_\nu(0\leqq\nu\leqq p-1)$ and P_∞ of the complete non-singular model C_n of the function field $k(x, y)$. If P is a point of C_n and j is a positive integer, $V_j(P)$ stands for the j-th ramification group of P in the meaning of Weil [11]. We find that

$$(6)\qquad \begin{cases} V_1(P_\nu)=\omega^{-\nu}\langle\sigma\rangle\omega^\nu\,, \quad V_2(P_\nu)=\{1\}\,, \quad (0\leqq\nu\leqq p-1)\,, \\ V_1(P_\infty)=G\,, \quad V_2(P_\infty)=\cdots=V_{n+1}(P_\infty)=\langle\omega\rangle\,, \quad V_{n+2}(P_\infty)=\{1\}\,. \end{cases}$$

For the proof of this fact, refer to Artin [1]. Let ξ_ρ be the correspondence of C_n defined by an element ρ of the Galois group G, and let Δ be the diagonal of $C_n\times C_n$. We denote by $M_l(\xi_\rho)$ the l-adic representation of G on the Tate group $T_l(J_n)$ of the jacobian variety J_n of C_n, and denote by $i_P(\rho)$ for $\rho\neq 1$, the multiplicity of $P\times P$ in the intersection $\Delta\cdot\xi_\rho$. We quote the result of Weil [11].

LEMMA. *The trace of $M_l(\xi_\rho)$ is given by the formula:*

$$\mathrm{tr}\, M_l(\xi_\rho)=2-\sum_P i_P(\rho)\,, \quad (\rho\neq 1)$$
$$\mathrm{tr}\, M_l(\xi_1)=2g\,,$$

where g is the genus of C_n and equal to $(n-1)(p-1)/2$.

From this lemma and (6) we can prove that

$$\mathrm{tr}\, M_l(\xi_{\omega^\nu\sigma^\mu})=\begin{cases} 0\,, & \mu\not\equiv 0\ (\mathrm{mod}\ p-1)\,, \\ -(p-1)\,, & \mu\equiv 0\ (\mathrm{mod}\ p-1)\,,\quad \mu\not\equiv 0\ (\mathrm{mod}\ n(p-1))\,,\quad \nu=0\,, \end{cases}$$

$$\begin{cases} 1, & \mu\equiv 0 \pmod{p-1}, \quad \mu\not\equiv 0 \pmod{n(p-1)}, \quad 1\leqslant\nu\leqslant p-1, \\ -(n-1), & \mu\equiv 0 \pmod{n(p-1)}, \quad 1\leqslant\nu\leqslant p-1. \end{cases}$$

Recall that the irreducible characters of G are $\psi_\alpha(1\leqslant\alpha\leqslant n(p-1))$ and $\chi_\beta(1\leqslant\beta\leqslant n)$, so that

$$(7) \qquad \operatorname{tr} M_l(\xi_\rho)=\sum_{\alpha=1}^{n(p-1)} a_\alpha\psi_\alpha(\rho)+\sum_{\beta=1}^{n} b_\beta\chi_\beta(\rho),$$

where the coefficients a_α and b_β are known by the orthogonality relations of characters:

$$a_\alpha=\frac{1}{np(p-1)}\sum_{\rho\in G}\psi_\alpha(\rho^{-1})\operatorname{tr} M_l(\xi_\rho),$$

$$b_\beta=\frac{1}{np(p-1)}\sum_{\rho\in G}\chi_\beta(\rho^{-1})\operatorname{tr} M_l(\xi_\rho).$$

After tedious calculation we conclude that

$$(8) \qquad a_\alpha=0 \ (1\leqslant\alpha\leqslant n(p-1)), \quad b_\beta=1 \ (1\leqslant\beta\leqslant n-1), \quad b_n=0.$$

Therefore we have proved that

$$(9) \qquad \operatorname{tr} M_l(\xi_\rho)=\sum_{\beta=1}^{n-1}\chi_\beta(\rho).$$

We summarize this fact in

THEOREM. *The l-adic representation $M_l(\xi_\rho)$ of the automorphism group G is the direct sum of the absolutely irreducible representations $S_1, S_2, \cdots, S_{n-1}$, each appearing with the same multiplicity one.*

Now let us set $n=p^h-1$ ($h=1, 2, \cdots$). In this case the Schur index of S_1 is, by (5), equal to $p-1(>2)$. According to Theorem 3, the local index of $\mathrm{env}_Q(S_1)$ at a prime ideal $\mathfrak{p}|p$ of $\boldsymbol{Q}(\chi_1)=\boldsymbol{Q}\left(\exp\frac{2\pi i}{p^h-1}\right)$ is also equal to $p-1$. Hence the representation S_1 is not rational over $\boldsymbol{Q}_p$, so that by the above Theorem, the representation $M_l(\xi_\rho)$ of G is not rational over $\boldsymbol{Q}_p$. On the other hand,

$$(10) \qquad \operatorname{tr} \mathrm{M}_l(\xi_\rho)=2-2\cdot r(\rho)+\sum_{Q\in Y} a_Q,$$

where a_Q is the character of the *Artin representation* at a point Q of the covering $Y=C_{p^h-1}/G$ and r is the character of the regular representation of G (cf. Serre [9, Théorème 4]). It follows that *at least one of the Artin representations of the covering C_{p^h-1}/G is not rational over $\boldsymbol{Q}_p$.* Therefore we have found such examples for all characteristic $p>2$.

Tokyo Metropolitan University

References

[1] E. Artin, Algebraic numbers and algebraic functions, Lecture Notes by I. Adamson, Princeton and New York Universities, 1951.

[2] R. Brauer, On the algebraic structure of group rings, J. Math. Soc. Japan, **3** (1951), 237-251.

[3] A. H. Clifford, Representations induced in an invariant subgroup, Ann. of Math., **38** (1937), 533-550.

[4] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

[5] H. Davenport und H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math., **172** (1935), 151-182.

[6] W. Feit, Characters of finite groups, Benjamin, New York, 1967.

[7] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1949.

[8] P. Roquette, Realisierung von Darstellungen endlicher nilpotenter Gruppen, Arch. Math., **9** (1958), 241-250.

[9] J.-P. Serre, Sur la rationalité des représentations d'Artin, Ann. of Math., **72** (1960), 406-420.

[10] L. Solomon, The representation of finite groups in algebraic number fields, J. Math. Soc. Japan, **13** (1961), 144-164.

[11] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.

[12] T. Yamada, On the Davenport-Hasse curves, J. Math. Soc. Japan, **20** (1968), 403-410.

[13] T. Yamada, On the group algebras of metabelian groups over algebraic number fields, Osaka J. Math. (to appear).

(Received March 5, 1968)