LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

12

# THEORY OF GROUP CHARACTERS

BY

RICHARD BRAUER

Published by
KINOKUNIYA BOOK-STORE Co., Ltd.
Tokyo, Japan

LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

12

# Theory of Group Characters

By
Richard Brauer

Notes prepared by
T. Tsuzuku

in cooperation with
T. Nakayama
P. Fong, A. Mizutani, N. Ito

Published by
KINOKUNIYA BOOK STORE Co., Ltd.

## Preface

In 1959, late Professor Richard Brauer visited Japan and gave interesting lectures at several universities, including Kyoto University.

Though twenty years have passed since then, these valuable note, based on a series of his lectures at Nagoya University (March-April, 1959), have been kept unpublished.

In view of the mathematical value, we decided to publish these notes in the lecture notes series of Department of Mathematics, Kyoto University.

M. Nagata
June 1979

CONTENTS

# I. Preliminaries

## §1. Algebras and their representations

Let $G$ be a finite group. A representation of $G$ over a field $\Omega$ is a homomorphism of $G$ onto a group of automorphisms (non-singular linear transformations) of a vector sapce $X$ over $\Omega$, such that the identity element of $G$ is mapped onto the identity transformation. Such a representation of $G$ over $\Omega$ can be extended in a natural way to a representation of the group algebra $\Gamma=\Gamma(G,\Omega)$ of $G$ over $\Omega$; recall $\Gamma$ is an algebra over $\Omega$ having a linearly independent basis over $\Omega$ such that under the multiplication of $\Gamma$ the elements of the basis form a group isomorphic to $G$, and often identified with $G$. A representation of an algebra $\Gamma$ over $\Omega$ is a homomorphism of $\Gamma$ onto an algebra over $\Omega$ of endomorphisms (linear transformations) of a vector space $X$ over $\Omega$, such that the identity element of $\Gamma$, whose existence we assume, is mapped onto the identity transformation.

So we first consider a finite-dimensional algebra $\Gamma$ with identity over a field $\Omega$. Let $\mathsf{X}$ be a representation of $\Gamma$ by linear transformations in a vector space $X$ over $\Omega$. We will call $X$ the representation space or the representation module of $\mathsf{X}$. $X$ is then a $\Gamma$-module, finite-dimensional over $\Omega$. Conversely, any $\Gamma$-module $X$, which is finite-dimensional over $\Omega$, gives rise to a representation of $\Gamma$. If we take a basis, say $v_1, v_2, \cdots, v_n$ of $X$, then the transformations $\mathsf{X}(\sigma)$, $\sigma\in\Gamma$, assume matrix form; we then speak of the matrix form of the representation $\mathsf{X}$.

$$(1)\qquad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \sigma = X(\sigma) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \qquad \sigma \in \Gamma$$

The term representation often refers to such a matrix form of the representation. If $\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = P \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ is a second basis of $X$, where $P$ is a non-singular matrix in $\Omega$, then the matrix form with respect to the second basis is $PX(\sigma)P^{-1}$. This last matrix form is said to be equivalent to the first. Equivalent matrix representations can always be regarded as matrix forms of the same representation taken with respect to different bases of the representation space, and may thus be considered as essentially the same. More generally, two representation modules of $\Gamma$ give rise to equivalent matrix representations if and only if they are operator-isomorphic with $\Gamma$ as ring of operators.

A representation $X$ of $\Gamma$ is called reducible or irreducible according to whether its space $X$ does or does not have proper $\Gamma$-subspace. In the former case, with a suitable choice of basis of $X$, the matrix form of $X$ may be taken in a form

$$(2)\qquad X = \begin{pmatrix} X_1 & 0 \\ * & X_2 \end{pmatrix}$$

where $X_1$, $X_2$ are the representations defined by the subspace and the corresponding quotient space. Any representation may, when we passed to an equivalent one, be written in a form

$$
(3) \qquad X = \begin{pmatrix} X_1 & & & 0 \\ & X_2 & & \\ & & \ddots & \\ * & & & X_r \end{pmatrix}, \qquad r \geqq 1
$$

with irreducible $X_i$; the representations $X_1, \cdots, X_r$ are called the constituents of $X$, and are uniquely determined up to order and equivalence by the Jordan-Hölder theorem.

In case the part $*$ in (3) (with irreducible $X_i$) can be made 0, the representation $X$ is called completely reducible. This is the case if and only if the representation space $X$ is completely reducible, i.e. is a direct sum of irreducible $\Gamma$-subspaces.

If we consider $\Gamma$ itself as a right $\Gamma$-module, we obtain the so-called (right or first) regular representation of $\Gamma$. Since any irreducible $\Gamma$-module is isomorphic to a module of the form $\Gamma/\mathfrak{r}$ with a maximal right ideal $\mathfrak{r}$ of $\Gamma$, the regular representation contains any irreducible representation as a constituent.

If $\Lambda$ is an extension field of $\Omega$, we obtain an algebra $\Gamma_\Lambda = \Gamma \times_\Omega \Lambda$ by extending the coefficient domain from $\Omega$ to $\Lambda$. A representation $X$ of $\Gamma$ by linear transformation in an $\Omega$-space $X$ can be extended in a natural way to a representation $X_\Lambda$ of $\Gamma_\Lambda$ by linear transformations in the $\Lambda$-space $X_\Lambda = X \times_\Omega \Lambda$. When we wish to differentiate $X$ from its extended representation $X_\Lambda$, we will call $X$ a representation of $\Gamma$ over $\Omega$. An irreducible representation $X$ (or its representation module $X$) is called <u>absolutely irreducible</u> if $X_\Lambda$ is irreducible for every extension field $\Lambda$ of $\Omega$; equivalently, this amounts to the irreducibility of the $\Gamma_\Lambda$-module $X_\Lambda$ for every extension field $\Lambda$. If every irreducible representation of an algebra $\Gamma$ is absolutely irreducible, then $\Gamma$ is said to split. If $\Gamma_\Lambda$ splits, $\Lambda$ is said to be a splitting field of $\Gamma$.

An algebra $\Gamma$ over an algebraically closed field $\Omega$ always splits. For if $X$ is an irreducible $\Gamma$-moudule, then the $\Gamma$-endomorphism ring of $X$ coincides with $\Omega$, since on the one hand it is a division ring, and on the other hand it is finite-dimensional over $\Omega$ as a subring of the full matrix ring of degree $(X:\Omega)$ over $\Omega$. But it is well-known (see below) that an irreducible representation module is absolutely irreducible if (and only if) its endomorphism ring coincides with the ground field.

Hence for any coefficient field $\Omega$, any algebraically closed extension $\Lambda$ of $\Omega$ will be a splitting field of $\Gamma$. From this it follows that $\Gamma$ always has a splitting field which is of finite degree over $\Omega$. To see this, consider an algebraically closed algebraic extension $\overline{\Omega}$ of $\Omega$, and the finite number of coefficients in those matrices corresponding to a basis of $\Gamma$ in a complete system of mutually inequivalent irreducible representations of $\Gamma_{\overline{\Omega}}$.

The above criterion for the absolute irreducibility of an irreducible representation may be obtained as follows: We show that if $(v_1,\cdots,v_m)$ is any basis of an irreducible representation module $X$ over its endomorphism ring, then there are $m$ elements $\sigma_1,\cdots,\sigma_m$ in $\Gamma$ satisfying

$$v_\mu\sigma_\nu = \delta_{\mu\nu}v_\mu \qquad (\mu,\nu=1,\cdots,m).$$

Indeed, since $X=v_i\Gamma$ for each $i$ (and in fact $X=v\Gamma$ for any non-zero element $v$ in $X$), this implies the existence of an element $\sigma$ in $\Gamma$ transforming $v_1,\cdots,v_m$ to $m$ arbitrarily given elements in $X$.

Hence in case $\Omega$ is itself the endomorphism ring of $X$, the representation $X(\Gamma)$ consists of all $m\times m$ matrices over $\Omega$. Furthermore, by considering the number of elements in $X(\Gamma)$ linearly independent over $\Omega$, it follows that $X(\Gamma)$ is a full matrix ring whenever $X$ is absolutely irreducible.

The subset

(4) $N = \{\sigma \in \Gamma \mid X_i(\sigma) = 0$ for every irreducible representation $X_i$ of $\Gamma$ over $\Omega\}$

of $\Gamma$ is a nilpotent ideal, since $X(N)$ is nilpotent when $X$ is the regular representation (or any faithful representation) of $\Gamma$. Conversely, any nilpotent right ideal $\mathfrak{r}$ of $\Gamma$ is represented by 0 in any irreducible representation $X$ (since $X\mathfrak{r}\neq 0$ would imply $X\mathfrak{r}=X$ and $X\mathfrak{r}^t=X$ for $t=1,2,\cdots$). Hence $N$ is the largest nilpotent ideal in $\Gamma$; $N$ contains all nilpotent right ideals in $\Gamma$ and by symmetry, also all nilpotent left ideals in $\Gamma$. $N$ is called the <u>radical</u> of $\Gamma$.

If the regular representation (or any faithful representation) of $\Gamma$ is completely reducible, then evidently $N=0$. The converse is true too. Thus, if the radical $N$ of $\Gamma$ is 0 ($\Gamma$ is then said to be <u>semi-simple</u>), every simple (*i.e.* irreducible) right ideal $\mathfrak{r}$ of $\Gamma$ is idempotent and we can then prove that $\mathfrak{r}$ is generated by an idempotent element $e$ in $\Gamma$, $\mathfrak{r}=e\Gamma$. Any right ideal $\mathfrak{r}_0$ containing $\mathfrak{r}$ is the direct sum $\mathfrak{r}_0=\mathfrak{r}+\mathfrak{r}'$, where $\mathfrak{r}'=\{\sigma\in\mathfrak{r}_0 \mid e\sigma=0\}$; observe that for any $\sigma\in\mathfrak{r}_0$ we have $\sigma=e\sigma+(\sigma-e\sigma)$, where $e\sigma\in\mathfrak{r}$ since $e\in\mathfrak{r}$, and $\sigma-e\sigma\in\mathfrak{r}'$. It follows readily that $\Gamma$ is a direct sum

(5) $$\Gamma = \mathfrak{r}_1 + \cdots + \mathfrak{r}_r$$

of simple right ideals $\mathfrak{r}_i$. If $X$ is any $\Gamma$-module, then $X=X\Gamma$ is the sum of subspaces $u\mathfrak{r}_i (u \in X)$. As an image of $\mathfrak{r}_i$, each $u\mathfrak{r}_i$ is either 0 or irreducible. Thus any $\Gamma$-module $X$ is completely reducible.

It is also well-known that under the same assumption of semi-simplicity, $N=0$, $\Gamma$ is a direct sum of simple (two-sided) ideals which are themselves simple algebras:

(6) $$\Gamma = \Gamma_1 + \cdots + \Gamma_n.$$

This decomposition is even unique up to the order of the summands. If $\mathfrak{r}$ is a simple right ideals, then $\Gamma\mathfrak{r}$ is a sum of right ideals isomorphic to $\mathfrak{r}$; thus the sum of all right ideals isomorphic to $\mathfrak{r}$ and contained in an ideal is again an ideal. Thus all simple right ideals contained in each component $\Gamma_i$ are isomorphic. It is evident that two simple right ideals contained in two distinct components, say $\Gamma_i$, $\Gamma_j$ $(i \neq j)$, are not isomorphic. Hence the components $\Gamma_i$ are in 1-1 correspondence with the distinct irreducible representations of $\Gamma$ (in $\Omega$). If

(7) $$1 = \varepsilon_1 + \cdots + \varepsilon_n, \qquad \varepsilon_i \in \Gamma_i,$$

is the decomposition of 1 according to (6), then $\varepsilon_1, \cdots, \varepsilon_n$ are idempotents belonging to the center $Z$ of $\Gamma$. $Z$ decomposes into the direct sum

(8) $$Z = Z_1 + \cdots + Z_n, \qquad Z_i = \varepsilon_i Z.$$

Each $Z_i$ is the center of $\Gamma_i$ and as such, is a simple commutative algebra, *i.e.* a field. In case the irreducible representation

$X_i$ corresponding to the component $\Gamma_i$ is absolutely irreducible, then $\Gamma_i \simeq X_i(\Gamma_i)$ is a full matrix algebra over $\Omega$, and $Z_i \simeq \Omega$. Under the same assumption of absolute irreducibility of $X_i$, the regular representation of $\Gamma$ contains the constituent $X_i$ as many times as the degree $x_i$ of $X_i$, since $\Gamma_i$ as a full matrix algebra of degree $x_i$, is then a direct sum of $x_i$ simple right ideals.

If $\Gamma$ is not semi-simple, the above considerations for the semi-simple case can be applied to the residue algebra $\Gamma/N$ of $\Gamma$ modules its radical $N$. For example, irreducible representations of $\Gamma$ in $\Omega$ are in 1-1 correspondence with simple ideal components of the residue algebra $\Gamma/N$, and an extention $\Lambda$ of $\Omega$ is a splitting field for $\Gamma$ if and only if $\Lambda$ is one for $\Gamma/N$. Furthermore, if $\Gamma$ is a commutative algebra, then the residue algebra $\Gamma/N$ is a direct sum of fields and every absolutely irreducible representation of $\Gamma$ is linear, *i.e.* of degree 1.

Given a representation $X$ of an algebra $\Gamma$, the mapping

$$\chi : \sigma \to \chi(\sigma) = \mathrm{Tr} X(\sigma)$$

is called the character of $\Gamma$ associated with the representation $X$, or more simply, the character of $X$. If $X$ is of degree 1, then the corresponding character is said to be linear. Hence a linear character in $\Omega$ is just a homomorphism of the algebra $\Gamma$ into $\Omega$.

We close this preparatory section with the following lemma which will be used in III, §1 below.

LEMMA 1. *Let $\Gamma$ be a splitting commutative algebra over $\Omega$, and $B$ a subalgebra of $\Gamma$. Then any linear character of $B$ in $\Omega$*

*may be extended to a character of* $\Gamma$ *in* $\Omega$.

PROOF. Consider the restriction $X|B$ to $B$ of the regular representation $X$ of $\Gamma$. Since all irreducible constituents of $X$ are linear, it is evident that the irreducible constituents of $X|B$ are all linear and are the restrictions to $B$ of the irreducible constituents of $X$. But the regular representation $Y$ of $B$ is contained in $X|B$. It follows that every irreducible representation of $B$ in $\Omega$ is linear and is the restriction of some linear representation of $\Gamma$.

## §2. Representations of finite groups — classical theory

Let $G$ be a finite group. For any field $\Omega$, the group algebra $\Gamma=\Gamma(G,\Omega)$ of $G$ over $\Omega$ has been defined before. $\Gamma$ consists of all linear combinations

$$\alpha = \sum_{G\in G} a_G G$$

of the elements $G$ of $G$ with coefficients $a_G$ in $\Omega$, when we identify a suitable basis of $\Gamma$ with $G$ itself. Every representation of $G$ in $\Omega$ can be uniquely extended to one of $\Gamma$, and conversely every representation of $\Gamma$ in $\Omega$ induces one of $G$. Notions concerning representations of algebras as in §1 can readily be transferred to those concerning representations of a group by this correspondence. In particular, with every class of equivalent representations of $G$ a character is associated. It is readily seen that a character takes the same value on conjugate elements of $G$ and is thus a function on the classes of conjugate elements of $G$. By using the elements of $G$ as basis elements, the regular representation of $G$ may be defined in a manner independent of the coefficient field $\Omega$. Its character is given by

$$\chi(G) = \begin{cases} g & G = 1 \\ 0 & G \neq 1, \end{cases} \tag{9}$$

where 1 is the unit element of $G$ and $g$ is the order of $G$.

PROPOSITION 1. *If the characteristic* $\mathrm{ch}\Omega$ *of* $\Omega$ *is prime to the order* $g$ *of* $G$, *then the group algebra* $\Gamma=\Gamma(G,\Omega)$ *is semi-simple, and hence every representation of* $G$ *over* $\Omega$ *is completely reducible.*

PROOF. Let $\lambda$ be the $\Omega$-linear map of $\Gamma$ to $\Omega$ defined by

$$\lambda\left(\sum_{G\in G} a_G G\right) = a_1,$$

where 1 is the unit element of $G$. If $\alpha=\sum a_G G$ is a non-zero element of $\Gamma$, then $a_{G_0}\neq 0$ for some $G_0 \in G$, and hence $\lambda(\alpha G_0^{-1})=a_{G_0}\neq 0$. It follows that if $\mathfrak{r}$ is a non-zero right ideal of $\Gamma$, then $\lambda(\mathfrak{r})\neq 0$, and $g\lambda(\mathfrak{r})\neq 0$. Now

$$g\lambda(G) = \begin{cases} g & G = 1 \\ 0 & G \neq 1. \end{cases}$$

Hence $g\lambda$ coincides with the character of the regular representation of $\Gamma$ given in (9), and hence $g\lambda(N)=0$ for the radical $N$ of $\Gamma$. This implies by the above remark that $N=0$. Hence $\Gamma$ is semi-simple.

If $\sum_G a_G G$ is an element of the center $Z=Z(G,\Omega)$ of $\Gamma=\Gamma(G,\Omega)$, then $a_G = a_{HGH^{-1}}$ for all $G$, $H \in G$; conversely, such elements of $\Gamma$ are in $Z$. Hence, if

$$K_1, K_2, \cdots, K_k$$

are the conjugate classes of G, and if for each $i=1,2,\cdots,k$, $K_i$ denotes the sum

$$K_i = \sum_{G \in K_i} G$$

of the elements in $K_i$, then the center $Z(G,\Omega)$ of $\Gamma(G,\Omega)$ is the set of linear combinations

$$\sum_{i=1}^{k} c_i K_i, \qquad c_i \in \Omega$$

of $K_i$, $i=1,\cdots,k$, over $\Omega$. For this reason $Z$ is thus called the class algebra of $G$ over $\Omega$. If ch$\Omega$ is prime to the order $g$ of G, then $\Gamma(G,\Omega)$ is semi-simple by the above proposition; its center $Z(G,\Omega)$ is also semi-simple and is thus a direct sum of fields, as was seen in the preceding section. If, moreover, $\Omega$ is algebraically closed, then these fields are all isomorphic to $\Omega$; their number is necessarily equal to the rank $k$ of $Z(G,\Omega)$ over $\Omega$. By our considerations of the preceding section, we have

PROPOSITION 2. *Let* ch$\Omega$ *be prime to g. The number of distinct (i.e. inequivalent) irreducible representations of* G *in an algebraically closed field over* $\Omega$ *is equal to the number k of conjugate classes of* G.

In particular, if $\Omega$ is an algebraically closed field of characteristic 0 (*e.g.* the field of all algebraic numbers or the field of all complex numbers), or more generally, if $\Omega$ is a splitting field of $G$ of characteristic 0, then there are exactly $k$ distinct absolutely irreducible representations

$$X_1, X_2, \cdots, X_k$$

of $G$ in $\Omega$. Their characters

$$\chi_1, \chi_2, \cdots, \chi_k$$

are simply called the irreducible characters of $G$.

PROPOSITION 3. *The irreducible characters* $\chi_1, \cdots, \chi_k$ *of* $G$ *satisfy the orthogonality relation*

$$\frac{1}{g} \sum_{G \in G} \chi_i(G)\chi_j(G^{-1}) = \delta_{ij}. \tag{10}$$

PROOF. Let $\chi$ denote the character of the regular representation of $G$. By our considerations in §1, we have

$$\chi(G) = \sum_{i=1}^{k} x_i \chi_i(G)$$

where $x_i = \chi_i(1)$ is the degree of $\chi_i$ (*i.e.* of $X_i$). Now $\chi$ is given by (9) as well. Hence for any two elements $G$, $H$ of $G$, we have, on setting $X_i(G) = (a_{\mu\nu}^{(i)}(G))$,

$$\delta_{G,H} = \frac{1}{g}\chi(GH^{-1}) = \frac{1}{g}\sum_{i=1}^{k} x_i \chi_i(GH^{-1})$$

$$= \sum_{i=1}^{k} \sum_{\mu=1}^{x_i} \frac{x_i}{g} a_{\mu\mu}^{(i)}(GH^{-1}) = \sum_{i=1}^{k} \sum_{\mu,\nu=1}^{x_i} a_{\mu\nu}^{(i)}(G) \frac{x_i}{g} a_{\nu\mu}^{(i)}(H^{-1}).$$

If we set

$$A = (a_{\mu\nu}^{(i)}(G))_{G,(i;\mu,\nu)}, \quad B = (\frac{x_i}{g} a_{\nu\mu}^{(i)}(G^{-1}))_{(i;\mu,\nu),G},$$

this relation may be expressed as

$$AB = I,$$

where $I$ denotes the identity matrix of degree $g$. The matrices $A$, $B$ are square matrices, since $g=\sum_{i=1}^{k} x_i^2$, and this implies

$$BA = I,$$

this is, however, nothing else but the orthogonality relation (10).

A function on $G$ is called a <u>class function</u> if it is constant on each conjugate class of $G$. Such a function is thus essentially a function of conjugate classes of $G$, and as was remarked before, examples of such are characters of $G$. The totality $A$ of class functions on $G$ in a field $\Omega$ forms a $k$-dimensional vector space over $\Omega$. In $A$ we can introduce an $\Omega$-bilinear inner product

$$(11) \qquad (\theta,\psi) = \frac{1}{g} \sum_{G\in G} \theta(G)\psi(G^{-1}).$$

In the case of a splitting field $\Omega$ of characteristic 0, the orthogonality relation (10) can be expressed simply as

$$(12) \qquad (\chi_i,\chi_j) = \delta_{ij}.$$

It follows in particular that the $k$ irreducible characters $\chi_1$, $\cdots$, $\chi_k$ are $\Omega$-linearly independent and form a basis of $A$. Every element $\theta$ of $A$ (*i.e.* every class function $\theta$ of $G$ in $\Omega$) may be written as a linear combination

$$(13) \qquad \theta = \sum_{i=1}^{k} a_i\chi_i, \qquad a_i \in \Omega$$

of $\chi_1,\cdots, \chi_k$; each coefficient $a_i$ is determined by

$$(14) \qquad a_i = (\theta,\chi_i).$$

$\theta$ is a character if and only if $a_i$ $(i=1,\cdots,k)$ are non-negative integers.

The orthogonality relation (10) may be expressed also as $\frac{1}{g}\sum_{\kappa=1}^{k}\frac{g}{c(G_\kappa)}\chi_i(G_\kappa)\chi_j(G_\kappa^{-1})=\delta_{ij}$, or

$$\sum_{\kappa=1}^{k}\frac{1}{c(G_\kappa)}\chi_i(G_\kappa)\chi_j(G_\kappa^{-1})=\delta_{ij}, \tag{15}$$

where $G_1,\cdots, G_k$ are representatives of the $k$ conjugate classes $K_1,\cdots, K_k$ of $G$, and $c(G)$ denotes the order of the centralizer in $G$ of the element $G$. If we set

$$X=(\chi_i(G_j)),\ \tilde{X}=(\chi_i(G_j^{-1})) \qquad (i,j=1,\cdots,k)$$

$$N=\begin{pmatrix} c(G_1) & & 0 \\ & \ddots & \\ 0 & & c(G_k)\end{pmatrix},$$

the relation (15) may be written as

$$XN^{-1}\tilde{X}'=I \tag{16}$$

where $X'$ is the transpose matrix of $X$. Hence also $N^{-1}\tilde{X}'X=I$, or

$$\tilde{X}'X=N. \tag{17}$$

PROPOSITION 4. *We have*

$$\sum_{i=1}^{k}\chi_i(G_\kappa)\chi_i(G_\lambda^{-1})=c(G_\kappa)\delta_{\kappa\lambda}, \tag{18}$$

*where* $\{G_\kappa,\ \kappa=1,\cdots,k\}$ *is a system of representatives of the* $k$ *conjugate classes of* $G$, *and* $c(G_\kappa)$ *is the order of the centralizer in* $G$ *of* $G_\kappa$.

Now let $\zeta$ be an element of the center $Z(G,\Omega)$ of $\Gamma(G,\Omega)$, where $\Omega$ is again a splitting field of $G$ of characteristic 0.

For each irreducible representation $X_i$ of $G$ over $\Omega$, the matrix $X_i(\zeta)$ is a scalar matrix

$$X_i(\zeta) = \omega_i(\zeta)I,\ \omega_i(\zeta) \in \Omega,$$

where $I$ is the identity matrix of degree $x_i$. Clearly $\omega_i$ is a linear character of $Z(G,\Omega)$. Furthermore, if as before $K_\kappa$ denotes the sum of elements in the conjugate class $K_\kappa$ of $G$, and if $G_\kappa$ is a representative of $K_\kappa$, then we have on computing the trace of $X_i(K_\kappa)=\omega_i(K_\kappa)I$ the equation $\frac{g}{c(G_\kappa)}\chi_i(G_\kappa)=x_i\omega_i(K_\kappa)$, *i.e.*

$$\omega_i(K_\kappa) = \frac{g}{c(G_\kappa)}\,\frac{\chi_i(G_\kappa)}{x_i}. \tag{19}$$

This formula shows that the $k$ linear characters $\omega_i$ $(i=1,\cdots,k)$ of $Z(G,\Omega)$ are linearly independent over $\Omega$, and since $(Z(G,\Omega):\Omega)=k$, they are all the linear characters of $Z(G,\Omega)$. We have also

PROPOSITION 5. *If $\zeta \in Z(G,\Omega)$ and $\omega_i(\zeta)=0$ for all $i=1,\cdots,k$, then $\zeta=0$. In particular, if $\zeta_1$, $\zeta_2 \in Z(G,\Omega)$ and $\omega_i(\zeta_1)=\omega_i(\zeta_2)$ for all $i=1,\cdots,k$, then $\zeta_1=\zeta_2$.*

Next, for each $\chi_i$ consider the element

$$\varepsilon_i = \frac{x_i}{g}\sum_{\kappa=1}^{k}\chi_i(G_\kappa^{-1})K_\kappa \tag{20}$$

of $Z(G,\Omega)$. Then

$$\begin{aligned}\omega_i(\varepsilon_j) &= \frac{x_j}{g}\sum_{\kappa=1}^{k}\chi_j(G_\kappa^{-1})\omega_i(K_\kappa)\\ &= \frac{x_j}{g}\sum_{\kappa=1}^{k}\chi_j(G_\kappa^{-1})\,\frac{g}{c(G_\kappa)}\,\frac{\chi_i(G_\kappa)}{x_i} = \frac{x_j}{x_i}(\chi_i,\chi_j) = \delta_{ij}.\end{aligned} \tag{21}$$

As $\omega_i$ is a linear character, we have

$$\omega_i(\varepsilon_j\varepsilon_\ell) = \omega_i(\varepsilon_j)\omega_i(\varepsilon_\ell) = \delta_{ij}\delta_{i\ell} = \delta_{ij}\delta_{j\ell} = \omega_i(\delta_{j\ell}\varepsilon_j).$$

Since this is the case for every $i$, we have

$$\varepsilon_j\varepsilon_\ell = \delta_{j\ell}\varepsilon_j. \tag{22}$$

Thus $\varepsilon_1,\cdots,\varepsilon_k$ are mutually orthogonal idempotents in $Z(G,\Omega)$; they are non-zero, as either the expression (20) or the relation (21) shows. Furthermore, since

$$\omega_i(\sum_{i=1}^{k}\varepsilon_j) = \sum_j \delta_{ij} = \omega_i(1)$$

for every $i=1,\cdots,k$, we have by Proposition 5

$$1 = \sum_{i=1}^{k}\varepsilon_i. \tag{23}$$

This relation (23) can also be seen from the fact that $k$ is the maximal number of mutually orthogonal idempotents in $Z(G,\Omega)$. This same observation also shows that each idempotent $\varepsilon_i$ is primitive. Thus (23) is the unique decomposition of 1 into mutually orthogonal primitive idempotents in $Z(G,\Omega)$. We have accordingly the direct decompositions

$$Z(G,\Omega) = \sum_{i=1}^{k}\varepsilon_i Z(G,\Omega)$$

$$\Gamma(G,\Omega) = \sum_{i=1}^{k}\varepsilon_i \Gamma(G,\Omega).$$

Here each $\varepsilon_i Z(G,\Omega)$ is isomorphic to $\Omega$ and $\varepsilon_i\Gamma(G,\Omega)$ is a complete matrix algebra of degree $x_i$ over $\Omega$.

Furthermore,

$$\omega_i(K_\kappa\varepsilon_j) = \omega_i(K_\kappa)\omega_i(\varepsilon_j) = \frac{g}{c(G_\kappa)}\frac{\chi_i(G_\kappa)}{x_i}\delta_{ij}.$$

But we also have

$$\omega_i\left(\frac{1}{c(G_\kappa)}\chi_j(G_\kappa)\sum_\lambda \chi_j(G_\lambda^{-1})K_\lambda\right)$$

$$= \frac{1}{c(G_\kappa)}\chi_j(G_\kappa)\sum_\lambda \chi_j(G_\lambda^{-1})\frac{g}{c(K_\lambda)}\frac{\chi_i(G_\lambda)}{x_i}$$

$$= \frac{1}{c(G_\kappa)}\chi_j(G_\kappa)\frac{g}{x_i}(\chi_i,\chi_j) = \frac{g}{c(G_\kappa)}\frac{\chi_i(G_\kappa)}{x_i}\delta_{ij}.$$

Since this is the case for all $i=1,\cdots,k$, we have

$$K_\kappa \varepsilon_j = \frac{1}{c(G_\kappa)}\chi_j(G_\kappa)\sum_\lambda \chi_j(G_\lambda^{-1})K_\lambda. \tag{24}$$

In the general case of a field $\Omega$ of characteristic 0 which is not necessarily a splitting field, we remark that the vector space $A(G)$ of all class functions on $G$ in $\Omega$ is not only a vector space with an inner product defined by (11), but also a commutative $\Omega$-algebra under the usual multiplication $(\theta\psi)(G)=\theta(G)\psi(G)$. Let $H$ be a subgroup of $G$. The restriction mapping $\theta\to\theta_H=\theta|H$ is clearly an $\Omega$-linear homomorphism of $A(G)$ into $A(H)$, the algebra of class functions on $H$ in $\Omega$. Furthermore, the identity element of $A(G)$ maps onto that of $A(H)$. In the reverse direction, for $\psi\in A(H)$, we have the induction mapping $\psi\to\psi^G$ defined by

$$\psi^G(G) = \frac{1}{h}\sum_{X\in G}\psi_0(XGX^{-1}), \tag{25}$$

where $h$ is the order of $H$, and $\psi_0(X)=\psi(X)$ or 0 according as $X\in H$ or not. For $\psi\in A(H)$, $\theta\in A(G)$ we have

$$\psi^G\theta = (\psi\theta_H)^G, \tag{26}$$

since $(\psi^G\theta)(G)=\psi^G(G)\theta(G)=\frac{1}{h}\sum_{X\in G}\psi_0(XGX^{-1})\theta(G)=\frac{1}{h}\sum_{\substack{X\in G\\ XGX^{-1}\in H}}(\psi\theta_H)(XGX^{-1})$ $=(\psi\theta_H)^G(G)$ (the third equality follows from the class property of $\theta$). We have also the Frobenius reciprocity

(27) $$(\psi^G,\theta) = (\psi,\theta_H),$$

where the right-hand side is the inner product in $A(H)$. For by (25)

$$(\psi^G,\theta) = \frac{1}{g}\sum_{G\in G}\psi^G(G)\theta(G^{-1}) = \frac{1}{g}\sum_{G\in G}\frac{1}{h}\sum_{X\in G}\psi_0(XGX^{-1})\theta(G^{-1})$$

$$= \frac{1}{gh}\sum_{\substack{X\in G\\ H\in H}}\psi(H)\theta(XH^{-1}X) = \frac{1}{h}\sum_{H\in H}\psi(H)\theta(H^{-1}) = (\psi,\theta_H).$$

It is evident that if $\theta$ is a character, then $\theta_H$ is one. Furthermore, replacing $\Omega$ by a suitable extension if necessary, and letting $\theta$ range over the irreducible characters $\chi_1,\cdots,\chi_k$ of $G$, we see that if $\psi$ is a character of $H$, then $\psi^G$ is one of $G$; $\psi^G$ is then called the <u>character of $G$ induced by $\psi$</u>. In fact, if $\psi$ is the character of a representation $Y$ of $H$, and if $G_1,\cdots,G_r$ form a system of representatives of the right cosets of $H$ in $G$, then $\psi^G$ is the character of the representation $X$ of $G$ constructed as follows;

(28) $$X(G) = \begin{pmatrix} Y(G_1GG_1^{-1})\cdots & & Y(G_1GG_r^{-1}) \\ & Y(G_\mu GG_\nu^{-1})\cdots & \\ Y(G_rGG_1^{-1})\cdots & & Y(G_rGG_r^{-1}) \end{pmatrix}$$

where we set $Y(G)=0$ whenever $G\notin H$; the representation $X$ of $G$ is said to be induced by $Y$. In terms of representation spaces, the space $X$ of $X$ has an $H$-subspace $Y$ defining the representation $Y$ of $H$ such that $X$ is the direct sum

(29) $$X = YG_1 + YG_2 + \cdots + YG_r.$$

Finally, if $X$ is a representation of $G$ and if we reduce by similarity transformations the matrix $X(G)$ representing an element $G$ of $G$ into triangular form in an algebraic closure of the ground field, then elements on the main diagonal are $(G)$-th roots of unity, where $(G)$ is the order of $G$, and hence a divisor of the order $g$ of $G$. If $\chi$ is the character of $X$, $\chi(G)$ is then the sum of these roots of unity. In particular, the values of a character are algebraic over the prime field. Instead of dealing with abstract fields algebraic over an abstract prime field of characteristic 0, we shall always work with fields of algebraic numbers, i.e. extensions of the rationals. Thus the values of a character in a field of characteristic 0 are all algebraic numbers, and are in particular, complex numbers. From the expression of $\chi(G)$ as a sum of roots of unity we then readily obtain

$$(30) \qquad \chi(G^{-1}) = \overline{\chi}(G), \qquad G \in G,$$

where $\overline{\chi}(G)=\overline{\chi(G)}$ is the complex conjugate of $\chi(G)$, the orthogonality relations (10), (15) may also be written as

$$(10') \qquad \frac{1}{g} \sum_{G \in G} \chi_i(G)\overline{\chi}_j(G) = \delta_{ij}$$

$$(15') \qquad \sum_{\kappa=1}^{k} \frac{1}{c(G_\kappa)} \chi_i(G_\kappa)\overline{\chi}_j(G_\kappa) = \delta_{ij}.$$

Also $\tilde{X}=\overline{X}$ and (18) becomes

$$(18') \qquad \sum_{i=1}^{k} \chi_i(G_\kappa)\overline{\chi}_i(G_\lambda) = c(G_\kappa)\delta_{\kappa\lambda}.$$

(24) becomes

(24')
$$K_\kappa \varepsilon_j = \frac{1}{c(G_\kappa)} \chi_j(G_\kappa) \sum_\lambda \overline{\chi}_j(G_\lambda) K_\lambda .$$

These suggest defining in the space of complex-valued class functions on $G$ an inner product

(31)
$$(\theta,\psi) = \frac{1}{g} \sum_{G\in G} \theta(G)\overline{\psi}(G)$$

in place of (11). This inner product is Hermitian, satisfies $(\theta,\psi)=\overline{(\psi,\theta)}$, and makes the space a Hilbert space. If $\psi$ is a linear combination of irreducible characters with real coefficients, then (11) and (31) coincide. In particular, (12), (13), and (14) are valid for this new and more natural inner product (31). Formula (27) is also valid, and can be proved either as before or from (26) and the relation $(\theta,\psi)=\frac{1}{g}\sum_{G\in G}(\theta\overline{\psi})(G)$.

§3. Cyclotomic splitting fields

In this section we will prove the existence of certain types of splitting fields for a finite group $G$. The proof, at the same time, establishes theorems on the generation of the characters of $G$ from those of certain subgroups of $G$, and these will be of use in later sections. As mentioned towards the end of the last section, we shall always deal with complex-valued characters rather than characters in abstract fields of characteristic 0; these we simply call characters. Let $A(G)$ be the space of all class functions on $G$ in the complex field $\Omega$. For any subring $S$ of $\Omega$ containing the ring $Z$ of rational integers, let $X_S(G)$ be the set of all linear combinations with coefficients in $S$ of the characters of $G$. $X_S(G)$ is then an $S$-module of $A(G)$, and since the product of two characters is again a character (being the character associated with the Kronecker product of the corresponding representations), $X_S(G)$ is a subring of $A(G)$. If $H$ is a subgroup of $G$, we define the ring $X_S(H)$ similarly.

Let $\{H_\alpha\}$ be a family of subgroups of $G$. We introduce $S$-modules $V_S$ and $U_S$ of $A(G)$ as follows: firstly,

$$V_S = \sum_\alpha X_S(H_\alpha)^G,$$

*i.e.* $V_S$ is the set of all $S$-linear combinations $\sum_{\alpha,j} a_{\alpha,j}\psi^G_{\alpha,j}$ with characters $\psi_{\alpha,j}$ of $H_\alpha$. Secondly $U_S$ is the set of all elements $\theta$ in $A(G)$ such that the restriction $\theta_{H_\alpha}$ belongs to $X_S(H_\alpha)$ for every $\alpha$. We will write $X_S$ for $X_S(G)$.

PROPOSITION 6. *$U_S$ is a subring of $A(G)$, $V_S$ is an ideal of $U_S$, and*

$$U_S \supseteq X_S \supseteq V_S.$$

PROOF. The first assertion is clear from the ring property of $X_S(H_\alpha)$. Every character of $G$ belongs to $U_S$ and this implies the first inclusion of the proposition. Since $\psi^G_{\alpha,j}$ is a character of $G$ for every character $\psi_{\alpha,j}$ of $H_\alpha$, we have the second inclusion as well. Furthermore, for any $\theta \in U_S$ we have $\theta_{H_\alpha} \in X_S(H_\alpha)$ and hence by (26),

$$\psi^G_{\alpha,j}\theta = (\psi_{\alpha,j}\theta_{H_\alpha})^G \in X_S(H_\alpha)^G \subseteq V_S$$

for every character $\psi_{\alpha,j}$ of $H_\alpha$. $V_S$ is thus an ideal of $U_S$.

The constant 1, being the unit character, belongs to $X_S$.

Its $S$-multiples $S$ can thus be considered as a subring of $X_S$.

LEMMA 2. *If the subring $S$ of $\Omega$ possesses a $Z$-basis, and if one of the basis elements is* 1, *then every rational integer $d$ in $V_S$ belongs to $V_Z$.*

PROOF. Let the $Z$-basis be $\{\eta_\mu\}$, say with $\eta_1=1$. The elements $\eta_\mu$ are then linearly independent over $X_Z$. To see this, suppose we have a relation $\sum_\mu \eta_\mu \theta_\mu = 0$ with $\theta_\mu \in X_Z$. Since every character is a sum of absolutely irreducible characters $\chi_1, \cdots, \chi_k$, such a relation can be written in the form $\sum_\mu \eta_\mu \sum_i a_{\mu i}\chi_i = 0$ with $a_{\mu i} \in Z$. But the $\chi_i$ are linearly independent over $\Omega$, so that $\sum_\mu \eta_\mu a_{\mu i} = 0$ for $i=1,\cdots,k$. Hence $a_{\mu i}=0$ for all $\mu$, $i$, and the $\eta_\mu$ are linearly independent over $X_Z$. Now if $d \in V_S \cap Z$, then

$$d\eta_1 = d = \sum_{\alpha, j} \psi^G_{\alpha, j} \sum_\mu z_{\alpha j \mu}\eta_\mu$$

with $\psi_{\alpha,j} \in X_S(H_\alpha)$ and $z_{\alpha j \mu} \in Z$. Comparing the coefficients of the basis element $\eta_1=1$ on both sides, we obtain $d \in V_Z$.

Now let $g$ be the order of $G$, and $\varepsilon$ a primitive $g$-th root of 1. We henceforth set $S=Z[\varepsilon]$. $S$ has a $Z$-basis of the form 1, $\varepsilon, \cdots, \varepsilon^{m-1}$ and hence Lemma 2 is applicable with this $S$.

LEMMA 3. *Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$ and assume $\mathfrak{H}$ is the direct product $\mathfrak{A}\times\mathfrak{B}$ of an abelian group $\mathfrak{A}$ of order $a$ and a group $\mathfrak{B}$ of order $b$, where $a$ and $b$ are relatively prime. Let $A$ be a fixed element of $\mathfrak{A}$, and let $\mathfrak{C}(A)$ be the centralizer of $A$ in $\mathfrak{G}$. Then there exists an element $\psi$ in $X_S(\mathfrak{H})$ such that $\psi^G(G) \in Z$ for every $G \in \mathfrak{G}$, $\psi^G(G)=0$ if $G$ is not conjugate in $\mathfrak{G}$ to an element of*

$AB$, *and* $\psi^G(A)=(C(A):B)$.

PROOF. Each linear character $\lambda_\nu$ of $A$ can be extended to a linear character $\omega_\nu$ of $H=A\times B$, where $\omega_\nu(B)=1$ for $B\in B$. Set

$$\psi = \sum_\nu \omega_\nu(A^{-1})\omega_\nu,$$

so that $\psi\in X_S(H)$. Since $A$ is abelian of order $a$, the orthogonality relations for the characters of $A$ show that $\psi(H)=a$ for $H\in AB$, and $\psi(H)=0$ for $H\in H$, $H\notin AB$. We now compute $\psi^G$ by (25). It is clear that $\psi^G(G)$ is a rational integer for every $G\in G$. If $G$ is not conjugate to an element of $AB$, the terms $\psi_0(XGX^{-1})$ in (25) all vanish, and hence $\psi^G(G)=0$. For $G=A$, we have $\psi_0(XAX^{-1})=a$ if $XAX^{-1}$ is an element $AB$ of $AB$, and $\psi_0(XAX^{-1})=0$ in all other cases. If $B\neq 1$, the order of $AB$ is not a divisor of $a$, and hence $AB$ cannot be conjugate to $A$. Thus $XAX^{-1}=AB$ holds only if $B=1$, and then $X$ must be in $C(A)$. Since the order $h$ of $H$ is $ab$, (25) yields

$$\psi^G(A) = (C(A):1)a/h = (C(A):1)/b = (C(A):B).$$

This proves our lemma.

Suppose that the subgroup $H=A\times B$ of Lemma 3 is contained in some member $H_\alpha$ of the family $\{H_\alpha\}$. Since the induction map in transitive,

$$\psi^G \in X_S(H_\alpha)^G \subseteq V_S.$$

We now show

PROPOSITION 7. *If the subgroups* $H_\alpha$ *of the family* $\{H_\alpha\}$ *cover* $G$, *then* $V_S$ *contains every class function* $\theta\in A(G)$ *whose values belong to* $gS$.

PROOF. Let $A$ be an element of a given conjugate class $K$ of

$G$, and let $H_\alpha$ contain $A$. Apply the above lemma to the case where A is the cyclic group generated by $A$ and where $B=\{1\}$. $V_S$ then contains the class function $\phi$ which is 0 outside $K$ and which takes the value $(C(A):1)$ on $K$. Since $(C(A):1)$ divides $g$, it follows that if $\theta$ satisfies the assumptions of the proposition, then $\theta$ is a linear combination with coefficients in $S$ of the various functions $\phi$ associated with the different classes $K$ of $G$. Hence $\theta \in V_S$.

Combining Proposition 7 with Lemma 2, we have the

COROLLARY. *If the subgroups $H_\alpha$ cover $G$, then $g \in V_Z$.*

Let $p$ be a fixed prime number. We call an element of $G$ <u>$p$-regular</u> or <u>$p$-singular</u> according as to whether or not its order is prime to $p$. An element whose order is a power of $p$ is called a <u>$p$-element</u>. A conjugate class of $G$ is then $p$-regular, $p$-singular, or a $p$-class if it consists respectively of $p$-regular elements, $p$-singular elements, or $p$-elements.

Every element $G$ of $G$ can be uniquely expressed as a commutative product

$$G = RP = PR \tag{32}$$

of a $p$-regular element $R$ and a $p$-element $P$, where $R$ and $P$ are both powers of $G$. To prove this, express the order $m$ of $G$ as a product $m=p^\mu m_0$, where $(p,m_0)=1$. There are then rational integers $s$ and $t$ with $1=sp^\mu+tm_0$. We may then take $R=G^{sp^\mu}$, $P=G^{tm_0}$. $R$ and $P$ are called respectively the $p$-regular component and the $p$-component of $G$.

If $\theta$ is any element of $X_S$ such that $\theta(G)$ and $\theta(R)$ belong to $Z$, then

$$(33) \qquad \theta(G) \equiv \theta(R) \pmod{p}.$$

In order to prove this, it will be enough to do the case where $G$ is a cyclic group with $G$ as generator. But in this case the irreducible characters $\chi_i$ of $G$ are linear, and $\chi_i(G)=\chi_i(P)\chi_i(R)$. If $P$ has order $p^\mu$, this implies that $\chi_i(G)^{p^\mu}=\chi_i(R)^{p^\mu}$. Now $\theta$ has the form $\theta=\sum_i a_i\chi_i$, where $a_i\in S$. Raising this equation to the $p^\mu$-th power, we have

$$\theta(G)^{p^\mu} \equiv \sum_i a_i^{p^\mu}\chi_i(G)^{p^\mu} \equiv \sum_i a_i^{p^\mu}\chi_i(R)^{p^\mu} \equiv \theta(R)^{p^\mu} \pmod{pS}.$$

By Fermat's theorem on the other hand,

$$\theta(G)^{p^\mu} \equiv \theta(G),\ \theta(R)^{p^\mu} \equiv \theta(R) \pmod{p}.$$

Thus we have (33), since $pS\cap Z=pZ$.

We will call a group $H$ <u>$p$-elementary</u> if $H$ is the direct product $A\times B$ of a cyclic group $A$ of order prime to $p$ and a $p$-group $B$.

LEMMA 4. *If every $p$-elementary subgroup of $G$ is contained in a member $H_\alpha$ of the family $\{H_\alpha\}$, then there exists an element $\eta$ of $V_S$ such that $\eta(G)\in Z$ and*

$$\eta(G) \equiv 1 \pmod{p}$$

*for every $G\in G$.*

PROOF. Let $\{A\}$ be a complete system of representatives for the $p$-regular classes of $G$. To prove the lemma it will be sufficient to construct an element $\eta_A$ of $V_S$ for every $A\in\{A\}$ with the following properties:

i) $\eta_A(G) \in Z$ for every $G \in \mathfrak{G}$,

$$\text{ii)}\quad \eta_A(G)\begin{cases} \equiv 1 & (\mathrm{mod}\ p) \text{ if the } p\text{-regular component of } G \text{ is conjugate to } A \text{ in } \mathfrak{G} \\ = 0 & \text{otherwise.} \end{cases}$$

For if such $\eta_A$ are obtained, we can take $\eta$ to be the sum $\sum_A \eta_A$. Hence fix $A \in \{A\}$, and let $\mathfrak{A}$ be the cyclic group generated by $A$. Let $\mathfrak{B}$ be a Sylow $p$-subgroup of the centralizer $\mathfrak{C}(A)$ of $A$, and set $\mathfrak{H} = \mathfrak{A} \times \mathfrak{B}$. $\mathfrak{H}$ is $p$-elementary and hence is contained in some $\mathfrak{H}_\alpha \in \{\mathfrak{H}_\alpha\}$. By Lemma 3 there is an element $\phi$ of $V_S$ such that $\phi(G) \in Z$ for every $G \in \mathfrak{G}$, $\phi(G) = 0$ if $G$ is not conjugate to an element of $A\mathfrak{B}$, and $\phi(A) = (\mathfrak{C}(A):\mathfrak{B})$. Since $(\mathfrak{C}(A):\mathfrak{B})$ is prime to $p$, there is a $z \in Z$ such that $z(\mathfrak{C}(A):\mathfrak{B}) \equiv 1 \pmod p$. If we set $\eta_A = z\phi$, then $\eta_A \in V_S$, and $\eta_A$ has the required properties i), ii). Indeed, i) is evident. Furthermore, if the $p$-regular component of $G$ is not conjugate to $A$ in $\mathfrak{G}$, then $G$ is not conjugate to an element of $A\mathfrak{B}$, and hence $\phi$ and $\eta_A$ vanish on $G$. On the other hand, we have $\eta_A(A) \equiv 1 \pmod p$. The remark made before this lemma shows that $\eta_A(G) \equiv 1 \pmod p$ if the $p$-regular component of $G$ is conjugate to $A$.

PROPOSITION 8. *If every $p$-elementary subgroup of $\mathfrak{G}$ is contained in some group $\mathfrak{H}_\alpha$ of the family $\{\mathfrak{H}_\alpha\}$, then $g_0 \in V_Z$, where $g = p^a g_0$ and $(g_0, p) = 1$.*

PROOF. Let $\eta$ be as in the above lemma. If $c$ is a rational integer such that $c \equiv 1 \pmod{p^j}$ for some $j = 1, 2, \cdots$, then $c^p \equiv 1 \pmod{p^{j+1}}$. It then follows that

$$\eta^{p^{a-1}}(G) \equiv 1 \qquad (\mathrm{mod}\ p^a)$$

for all $G\in G$. Since $V_S$ is an ideal and hence a ring, $\eta^{p^{a-1}}\in V_S$. Set $\eta^{p^{a-1}}=1+\theta_0$. The above congruence shows that Proposition 7 can be applied to the class function $\theta=g_0\theta_0$. It follows that $g_0\theta_0\in V_S$ and hence $g_0=g_0\eta^{p^{a-1}}-g_0\theta_0\in V_S$. By Lemma 2 $g_0\in V_Z$.

We will call a group elementary if it is $p$-elementary for some prime $p$.

COROLLARY. *If every elementary subgroup of $G$ is contained in some member $H_\alpha$ of the family $\{H_\alpha\}$, then*

$$U_Z = X_Z(G) = V_Z \tag{34}$$

*and for any subring $S$ of the complex field containing $Z$ (not necessarily of the form $Z[\varepsilon]$),*

$$U_S = X_S(G) = V_S. \tag{35}$$

PROOF. Proposition 8 can be applied for every prime $p$, so that $V_Z$ contains a rational integer prime to $p$ for every prime number $p$. Thus $1\in V_Z$. Since $V_Z$ is an ideal of $U_Z$, this implies that $U_Z=V_Z$ and thus (34). Furthermore, since $V_S\supseteq V_Z$ we have $1\in V_S$, and hence (35).

If we take $\{H_\alpha\}$ to be the set of all elementary subgroups of $G$, we may express the equalities $X_Z(G)=V_Z$ and $X_Z(G)=U_Z$ as follows:

PROPOSITION 9. *Every (complex-valued) character $\chi$ of $G$ can be represented in the form*

$$\chi = \sum a_i\psi_i^* \tag{36}$$

*where each $\psi_i$ is an irreducible character of some elementary subgroup $E$ of $G$, $\psi_i^*$ is the character of $G$ induced by $\psi_i$, and each*

$a_i$ *is a rational integer.*

PROPOSITION 10. *A complex-valued function* $\theta$ *on* $G$ *is a generalized character of* $G$ *(i.e. a Z-linear combination of irreducible characters) if and only if the following two conditions are satisfied:*

i) $\theta$ *is a class function.*

ii) *For every elementary subgroup* $E$ *of* $G$, *the restriction* $\theta|E$ *to* $E$ *is a generalized character of* $E$.

In connection with Proposition 9 we note

LEMMA 5. *Every irreducible character* $\psi$ *of an elementary group* $E$ *is induced by a linear character of some subgroup.*

PROOF. The lemma is actually true for any nilpotent group $E$. By replacing $E$ by a subgroup if necessary, we need consider only the case where $\psi$ is primitive, *i.e.* $\psi$ is not induced by a character of some proper subgroup. Furthermore, by passing to a factor group, we may also assume that $\psi$ is the character of a faithful irreducible representation $X$ over the complex field $\Omega$. Let $X$ be the representation space of $X$. Let $A$ be an abelian normal subgroup of $E$. Since the group algebra $\Gamma(A,\Omega)$ is the direct sum of $(A:1)$ mutually orthogonal fields $\Gamma_\mu$ all isomorphic to $\Omega$, the $A$-module $X$ is the direct sum of the submodules $X\Gamma_\mu$, some of which may be 0. Each element $G$ of $E$ permutes by transformation the $\Gamma_\mu$ among themselves, and since $X\Gamma_\mu G = XGG^{-1}\Gamma_\mu G = XG^{-1}\Gamma_\mu G$, $G$ permutes by right multiplication the $X\Gamma_\mu$ among themselves. If we consider only the non-zero summands $X\Gamma_\mu$, then the permutation group effected among them is transitive. Because of the irreducibility of the $\Gamma(E,\Omega)$-module $X$, $X=\sum X\Gamma_\mu$. Let $X\Gamma_1$ be a non-zero summand among the $X\Gamma_\mu$, and let $E_1$ be the subgroup of $E$ consisting of all elements leaving $X\Gamma_1$ fixed. The representation $X$ is then induced by the representation of $E_1$ defined by $X\Gamma_1$. Because of the primitivity assumption on $\psi$, it follows that $E=E_1$ and $X=X\Gamma_1$. Hence the representation module $X$ of $A$ is a direct sum of irreducible modules, all of which are isomorphic to $\Gamma_1$ and of dimension 1 over $\Omega$. Thus the representation $X(A)$ consists of scalar matrices, and since $X$ is faithful, $A$ is contained in the center of $E$. Being a factor group of a subgroup of the original group, $E$ is nilpotent. This implies that $E$ itself is abelian. For if a maximal abelian normal subgroup $A$ of $E$ were smaller than $E$, then $E/A$ would contain a cyclic normal subgroup $\neq 1$, whose inverse image under the homomorphism $E\to E/A$ would be an abelian normal subgroup of $E$ larger than $A$, since $A$ is central. Thus $E$ is abelian and its irreducible character $\psi$ is linear (in fact $E$ is cyclic). This proves the lemma.

We now have the following refinement of Schur's conjecture.

PROPOSITION 11. *Let $m$ be the least common multiple of the orders of the elements of $G$, and let $K$ be the field of $m$-th roots of 1 over the rational field. Then $K$ is a splitting field of $G$, i.e. every irreducible representation of $G$ in $K$ is absolutely irreducible.*

PROOF. Let $X$ be an irreducible representation of $G$ over the complex field $\Omega$. $X$ is then contained as in irreducible constituent in an irreducible representation $Y$ of $G$ over $K$, say with multiplicity $s$. Since an irreducible representation of $G$ over $K$ contains $X$ if and only if it is equivalent to $Y$, the multiplicity of $X$ in any representation of $G$ over $K$ is always a multiple of $s$. The number $s$ is called the Schur index of $X$ with respect to $K$, and what we have to show is that $s=1$. Now $K$ contains the character $\chi$ of $X$, as well as the characters of every subgroup of $G$. In particular, if $\lambda$ is a linear character of a subgroup $H$ of $G$, and $\lambda^*$ is the character of $G$ induced by $\lambda$, then the representation corresponding to $\lambda^*$ is realizable in $K$. Indeed, we may simply take the representation of $G$ induced by the linear representation $\lambda$ of $H$. Express now $\chi$ in the form (36) of Proposition 9 with the $a_i$ and the $\psi_i$ as described there. If $p$ is any fixed prime, (36) shows that there exists at least one $\psi_i^*$ containing $\chi$ with a multiplicity $t$ relatively prime to $p$. By Lemma 5 $\psi_i$ is induced by a linear character of some subgroup of $E_i$. Since the process of induction is transitive, the character $\psi_i^*$ of $G$ is induced by a linear character of a subgroup, and hence corresponds to a representation of $G$ realizable in $K$. Since this representation contains $X$ $t$ times, the Schur index $s$ of $X$ with respect to $K$ divides $t$, and is thus relatively prime to $p$. This is the case for any prime $p$. Thus $s=1$.

Proposition 9 first appeared in [15] in connection with a problem of Artin. This result was then used to prove Schur's conjecture in [14]; the refinement as given in Proposition 11 appeared in [16]. Proposition 10 first appeared in [18]. Subsequent simplifications of the proofs of Propositions 9 and 10 can be found in [1] or [30]. For proofs differing considerably from those in the above references, we refer to the papers [33'] of Solomon and [33"] of Swan. For problems concerning the Schur index, see [17], [33], and [38].

The methods and results in this section have been rather more arithmetical than algebraic. Properties of group characters even more arithmetical will be studied in the following chapters.

In studying arithmetical properties of group representations it is often useful and necessary to consider group algebras over commutative rings which are not fields. The group algebra $\Gamma(G, \mathfrak{o})$ of $G$ over a commutative ring $\mathfrak{o}$ with an identity is defined in the same way as in the case of a group algebra over a field. Its center $Z(G,\mathfrak{o})$ consists of all linear combinations over $\mathfrak{o}$ of the sums $K_\lambda$ of elements of conjugate classes.

We close this chapter by mentioning a problem of some what arithmetical nature on group algebras. Let $G_1$, $G_2$ be two finite groups. Suppose that for every field $K$ of characteristic 0 or a prime number, the group algebras $\Gamma(G_1,K)$, $\Gamma(G_2,K)$ of $G_1$, $G_2$ over $K$ are isomorphic. Are then $G_1$ and $G_2$ isomorphic? Also, if the group rings $\Gamma(G_1,Z)$, $\Gamma(G_2,Z)$ over the rational integers $Z$ are isomorphic, are then $G_1$, and $G_2$ isomorphic?

## II. Arithmetical Structure

### §1. The numbers $\omega_i(K_\alpha)$

Let $\Omega$ be an algebraic number field, and let $\Omega_0$ be a subring with 1 of $\Omega$. The center $Z(G,\Omega_0)$ of the group ring $\Gamma(G,\Omega_0)$ over $\Omega_0$ is spanned over $\Omega_0$ by the sums $K_1,\cdots, K_k$ of the elements of the $k$ conjugate classes of $G$. Each of the $k$ functions $\omega_i$ (I,§2) maps $Z(G,\Omega_0)$ onto a subring of the field generated over $\Omega_0$ by the $g$-th roots of unity. Indeed the image is a finitely-generated $\Omega_0$-module, with generators $\omega_i(K_1),\cdots, \omega_i(K_k)$. It follows that the image consists of numbers integral over $\Omega_0$. Taking $\Omega_0$ to be any ring between the ring of rational integers and the ring of algebraic integers in $\Omega$, we have

PROPOSITION 1. *For each $\omega_i$ the numbers $\omega_i(K_1),\cdots, \omega_i(K_k)$ are algebraic integers.*

PROPOSITION 2. *For every irreducible character $\chi_i$ of $G$, the degree $x_i=\chi_i(1)$ divides the order $g$ of $G$.*

PROOF. By the orthogonality relation I, (15') we have $\sum_{\alpha=1}^{k}\frac{g}{c(G_\alpha)}\chi_i(G_\alpha)\chi_j(G_\alpha)=g\delta_{ij}$, *i.e.*

$$\sum_{\alpha=1}^{k} \omega_i(K_\alpha)\chi_j(G_\alpha) = \frac{g}{x_i}\,\delta_{ij}. \tag{1}$$

In particular $\sum_{\alpha=1}^{k}\omega_i(K_\alpha)\chi_i(G_\alpha)=\frac{g}{x_i}$. The left hand side is an algebraic integer by Proposition 1. The right hand side is a rational number. Hence the common value is a rational integer, proving $x_i|g$.

## §2. Modular representations and their characters

We now consider a fixed rational prime $p$. Let $p^a$ be the highest power of $p$ dividing the order $g$ of $G$, so that

(2) $$g = p^a g_0, \quad (p, g_0) = 1.$$

Let $\nu$ be a fixed extension to $\Omega$ of the $p$-adic exponential valuation of the rationals, normalized so that $\nu(p)=1$. Let $\mathfrak{o}$ be the ring of integers for $\nu$, and $\mathfrak{p}$ the unique prime (and in fact maximal) ideal of $\mathfrak{o}$: recall $\mathfrak{p}$ consists of those numbers with positive $\nu$-value. The residue class ring

(3) $$\Omega^* = \mathfrak{o}/\mathfrak{p}$$

is then a field of characteristic $p$. A representation of $G$ over the field $\Omega^*$ is called a modular representation of $G$.

From now on we shall assume that the algebraic number field $\Omega$ contains all of the $g$-th roots of 1 in some algebraic closure of the rationals. Let $E_0$ and $E_0^*$ be the group of all $g_0$-th roots of 1 in $\Omega$ and $\Omega^*$ respectively. If $\eta$ is in $E_0$, and $\eta^*$ denotes the residue class of $\eta$ (mod $\mathfrak{p}$), then the mapping $\eta \to \eta^*$ is an isomorphism of $E_0$ onto the group $E_0^*$. Indeed, if $\eta$, $\eta_1$ are two distinct elements of $E_0$, the quotient $\frac{\eta}{\eta_1}$ is a $g_0$-th root of 1 in $\Omega$ different from 1, *i.e.* a root of the polynomial $\frac{X^{g_0}-1}{X-1}$. Since $\left[\frac{X^{g_0}-1}{X-1}\right]_{x=1} = g_0$, we have $\frac{\eta}{\eta_1} - 1 \mid g_0$. This is possible only when $\frac{\eta}{\eta_1} \not\equiv 1$ (mod $\mathfrak{p}$), *i.e.* $\eta \not\equiv \eta_1$ (mod $\mathfrak{p}$), since $p \nmid g_0$. Thus the $g_0$ elements $\eta^*$, $\eta \in E_0$, are all distinct. They are evidently $g_0$-th roots of 1 in $\Omega^*$. Since there are at most $g_0$ $g_0$-th roots of 1 in $\Omega^*$, the mapping $\eta \to \eta^*$ is an isomorphism of $E_0$ onto $E_0^*$.

Now let $F$ be a modular representation of $G$, *i.e.* a representation of $G$ in the field $\Omega^*$, and let $f$ be its degree. Let $R$ be a $p$-regular element of $G$, and let $\varepsilon_1^*, \cdots, \varepsilon_f^*$ be the characteristic roots of $F(R)$. The $\varepsilon_i^*$ are $g_0$-th roots of 1 in $\Omega^*$. By the above remark there exists for each $\varepsilon_i^*$ one and only one $g_0$-th root of 1 in $\Omega$, say $\varepsilon_i$, whose residue class (mod $p$) is $\varepsilon_i^*$. We set

$$\phi(R) = \sum_{i=1}^{f} \varepsilon_i, \tag{4}$$

and call $\phi$ the character of the modular representation $F$ (or more simply a modular character). We remark that $\phi(R)$ is defined only for $p$-regular elements $R$, and that the value $\phi(R)$ belongs to $\Omega$ and not to $\Omega^*$.[1] The residue class $\phi(R)^*$ of $\phi(R)$ (mod $p$) is the trace tr $F(R) = \sum_{i=1}^{f} \varepsilon_i^*$ of $F(R)$.

## §3. Transition from an ordinary representation to a modular one

Representations over $\Omega$ (or more generally over a field of characteristic 0) will be called ordinary representations, and their characters ordinary characters in order to distinguish them from modular representations and their characters. Let $X$ be an ordinary representation of $G$ over $\Omega$, and $X$ its

---

1) It is known that two modular representations have the same irreducible constituents if and only if their characters coincide; see [25]. However, we may and shall proceed without assuming this.

representation module. Let $e_1, \cdots, e_x$ be an $\Omega$-basis of $X$. The $\mathfrak{o}$-module $M$ generated by the elements $e_\mu G$, $1 \leq \mu \leq x$, $G \in G$, has an $\mathfrak{o}$-basis $e'_1, \cdots, e'_y$, since it is finitely-generated. Indeed, if $e'_1, \cdots, e'_y$ are elements of $M$ such that $e'_1, \cdots, e'_y \pmod{pM}$ form an $\mathfrak{o}/\mathfrak{p}=\Omega^*$ basis of the finitely-generated $\mathfrak{o}/\mathfrak{p}$-module $M/\mathfrak{p}M$, then $e'_1, \cdots, e'_y$ generate $M$ over $\mathfrak{o}$ (since $\mathfrak{p}$ is the Jacobson radical of $\mathfrak{o}$), $e'_1, \cdots, e'_y$ are then evidently linearly independent over $\mathfrak{o}$ and over $\Omega$. Since the $\Omega$-module generated by $\{e_\mu G\}$ is $X$, we have $y=x$, and $e'_1, \cdots, e'_x$ form an $\Omega$-basis of $X$. If we consider the matrix form of X with respect to this new basis $e'_1, \cdots, e'_x$, all the matrices $X(G)$, $G \in G$, have coefficients in $\mathfrak{o}$. Passing to their residue classes $\pmod{\mathfrak{p}}$, we obtain a representation $X^*$ in $\Omega^*$. If we denote the $\mathfrak{o}$-$G$-module $\mathfrak{o}e'_1+\cdots+\mathfrak{o}e'_x$ by $X_0$, the modular representation $X^*$ corresponds to the representation module $X_0/\mathfrak{p}X_0$ over $\Omega^*$.

REMARK. *The representation* $X^*$ *depends on the choice of the* $\Omega$-*basis* $e_1, \cdots, e_x$ *of* $X$ *we started with, and hence is not uniquely determined by the representation* $X$.[1)]

## §4. Decomposition numbers and Cartan invariants

From now on we shall always assume that $\Omega$ and $\Omega^*$ are

---

1) If we use the result in the foot-note of the preceding page, it follows that the irreducible constituents of $X^*$ are uniquely determined by $X$. We shall give an alternative proof of this in §4.

splitting fields of $G$.[1] Let $F_1, \cdots, F_\ell$ be the totality of non-equivalent irreducible modular representations of $G$ (*i.e.* irreducible representations over $\Omega^*$). Let $\phi_1, \cdots, \phi_\ell$ be their characters and $f_1, \cdots, f_\ell$ their degrees. Let $X_1, \cdots, X_k$ be the totality of non-equivalent irreducible representations of $G$ over $\Omega$ (*i.e.* irreducible ordinary representations); the number $k$ is equal to the number of conjugate classes of $G$. Their characters and degrees are denoted as before by $\chi_1, \cdots, \chi_k$ and $x_1, \cdots, x_k$. Now construct a modular representation $X_i^*$ from each $X_i$, and denote the multiplicity of $F_\rho$ in $X_i^*$ by $d_{i\rho}$. The non-negative integers $d_{i\rho}$ ($i=1,\cdots,k$; $\rho=1,\cdots,\ell$) are called the decomposition numbers of $G$ (with respect to $p$). For a $p$-regular element $R$ we have

$$\chi_i(R) = \sum_{\rho=1}^{\ell} d_{i\rho}\phi_\rho(R). \tag{5}$$

For each $\rho=1,\cdots,\ell$ we define an ordinary character $\Phi_\rho$ by setting

$$\Phi_\rho(G) = \sum_{i=1}^{k} d_{i\rho}\chi_i(G), \qquad G \in G. \tag{6}$$

For $R$ $p$-regular we obtain from (5) and (6)

$$\Phi_\rho(R) = \sum_{\sigma=1}^{\ell} c_{\rho\sigma}\phi_\sigma(R), \qquad R \text{ } p\text{-regular}, \tag{7}$$

where

$$c_{\rho\sigma} = \sum_{i=1}^{k} d_{i\rho}d_{i\sigma} = c_{\sigma\rho}. \tag{8}$$

---

1) It is true that $\Omega^*$ is a splitting field of $G$ whenever $\Omega$ is. However, we can proceed without using this fact by taking $\Omega$ large enough at the beginning.

We call the non-negative integers $c_{\rho\sigma}$ $(\rho,\sigma=1,\cdots,\ell)$ the <u>Cartan invariants</u> of $G$ (with respect to $p$).[1] Let

$$D = (d_{i\rho})_{i=1,\cdots,k;\rho=1,\cdots,\ell}$$

$$C = (c_{\rho\sigma})_{\rho,\sigma=1,\cdots,\ell}$$

be the matrices of decomposition numbers and Cartan invariants. The last relation (8) may then be expressed in matrix form as

$$C = D'D. \tag{9}$$

Now by our considerations in I, §1 on absolutely irreducible representations and the decomposition of an algebra modulo its radical (essentially a lemma of Frobenius and Schur), there exists for each $\rho=1,\cdots,\ell$ an element $\gamma_\rho^*$ in $\Gamma(G,\Omega^*)$ such that if $F_1,\cdots, F_\ell$ are in matrix form, then

$$F_\rho(\gamma_\rho^*) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$F_\rho(\gamma_\sigma^*) = 0 \qquad \text{for } \sigma \neq \rho.$$

It follows that the traces $\phi_1^*,\cdots, \phi_\ell^*$ of $F_1,\cdots, F_\ell$ are linearly independent over $\Omega^*$. But each $\phi_\rho^*$ is determined by its values on $p$-regular elements. For if $G=RP=PR$ is the unique decomposition of $G$ into its $p$-regular component $R$ and its $p$-component $P$ (I,(32)),

---

1) They are in fact the Cartan invariants of the algebra $\Gamma(G,\Omega^*)$. The characters $\Phi_\alpha$ have an important significance for the algebra $\Gamma(G,\Omega^*)$; this was shown in [25] (cf. also [3], [31]). However, this will not be needed.

we have $F_\rho(G)=F_\rho(R)F_\rho(P)=F_\rho(P)F_\rho(R)$. Thus tr $F_\rho(G)=$tr $F_\rho(R)$, since the characteristic roots of $F_\rho(P)$, being $p^\mu$-th roots of 1 in $\Omega^*$, are all 1. Thus each $\phi^*_\rho$ is essentially a function of the $p$-regular classes of $G$. It follows that the number $\ell$ is at most equal to the number $\ell_0$ of $p$-regular classes of $G$, $\ell\le\ell_0$.

Since $\phi^*_1,\cdots,\phi^*_\ell$ are linearly independent over $\Omega^*$, and since they are essentially functions on the $p$-regular classes, we see that the $\ell$ modular character $\phi_1,\cdots,\phi_\ell$ are linearly independent over $o$ (mod $p$), and hence over $o$ itself (*i.e.* over $\Omega$). By (5) this yields

PROPOSITION 3. *The decomposition numbers $d_{i\rho}$, the Cartan invariants $c_{\rho\sigma}$, and the characters $\Phi_\rho$ do not depend on the choice of the bases in the representation modules $X_i$ from which the $X^*_i$ were constructed.*

REMARK. *For each $\chi_i$, there evidently exists at least one $\phi_\rho$ with $d_{i\rho}\neq 0$. By considering the regular representation, we can also see that for each $\phi_\rho$, there exists at least one $\chi_i$ with $d_{i\rho}\neq 0$. However, this will also be a consequence of (17) below.*

## §5. The number of irreducible modular characters

Consider the matrices

(10) $X_r=(\chi_i(G_\alpha))$ $\quad$ $i=1,\cdots,k$; $G_\alpha$ runs over a set of representatives of the $\ell_0$ $p$-regular classes $K_1,\cdots,K_{\ell_0}$ of $G$

and

(11) $$N_r = \begin{pmatrix} c(G_1) & & 0 \\ & \ddots & \\ 0 & & c(G_{\ell_0}) \end{pmatrix}$$

(the "$r$" refers to $p$-regular). We have by the orthogonality relation I, (18')

(12) $$X_r'\overline{X}_r = N_r.$$

Now

(13) $$X_r = D\phi$$

where $\phi$ is the $(\ell\times\ell_0)$-matrix

(14) $$\phi = (\phi_\rho(G_\alpha)) \qquad \begin{array}{l} \rho = 1,\cdots,\ell \\ K_\alpha \ p\text{-regular} \end{array}$$

of irreducible modular characters. Hence (12) reads $\phi'D'D\overline{\phi}=N_r$ or

(15) $$\phi'C\overline{\phi} = N_r.$$

The rank of the matrix on the left hand side is at most equal to $\ell$, while the rank of $N_r$ is evidently $\ell_0$ by (11). It follows $\ell \geqq \ell_0$. Combining this with the inequality obtained in the preceding section, we have

PROPOSITION 4.[1] *The number $\ell$ of irreducible modular characters of $G$ is equal to the number $\ell_0$ of $p$-regular classes of $G$,*

$$\ell = \ell_0.$$

The matrix $\phi$ in (14) is thus a square matrix of degree $\ell=\ell_0$,

1) This was first established in [2]. The present proof is similar to the one in [25]. For a third proof, see [26] as well as §7 below.

and since $\phi_1, \cdots, \phi_\ell$ are linearly independent (mod $p$),

(16) $$\det \phi \not\equiv 0 \pmod{p}.$$

From (15) we have furthermore[1])

(17) $$\det C \neq 0.$$

From (15) we also obtain $\overline{\phi}^{-1} C^{-1} \phi'^{-1} = N_r^{-1}$, or

(18) $$\overline{\phi} N_r^{-1} \phi' = C^{-1}.$$

This can also be expressed as

(19) $$C \overline{\phi} N_r^{-1} \phi' = I.$$

If we put $(\theta, \phi)_r = \sum_{K_\alpha\ p\text{-regular}} \frac{1}{c(G_\alpha)} \theta(G_\alpha) \overline{\phi}(G_\alpha)$ for any two class functions $\theta$, $\phi$ of $G$ defined on the $p$-regular classes, then (19) can also be written as

(20) $$(\phi_\rho, \sum_{\nu=1}^{\ell} c_{\sigma\nu} \phi_\nu)_r = \sum_{\nu=1}^{\ell} c_{\sigma\nu} (\phi_\rho, \phi_\nu)_r = \delta_{\rho\sigma}.$$

(20) implies that any class function $\theta$ of $G$ defined on $p$-regular classes is a linear combination $\theta = \sum_{\rho=1}^{\ell} a_\rho \phi_\rho$ of the $\phi_\rho$ with coefficients

(21) $$a_\rho = (\theta, \sum_{\sigma=1}^{\ell} c_{\rho\sigma} \phi_\sigma)_r = \sum_{\sigma=1}^{\ell} c_{\rho\sigma} (\theta, \phi_\sigma)_r.$$

## §6. The characters $\Phi_\rho$

The relation (15), (18), (19), and (20) are orthogonality relations for the irreducible modular characters. By (7) the

---

1) The value of $\det C$ will be determined in §11 below.

relation (15) can be written as

$$(15') \qquad \sum_{\rho=1}^{\ell} \phi_\rho(G_\alpha)\overline{\Phi}_\rho(G_\beta) = c(G_\alpha)\delta_{\alpha\beta}, \qquad K_\alpha,\ K_\beta\ p\text{-regular}$$

while (19), (20) can be written as

$$(19') \qquad \sum_{K_\alpha\ p\text{-regular}} \frac{1}{c(G_\alpha)} \phi_\rho(G_\alpha)\overline{\Phi}_\sigma(G_\alpha) = \delta_{\rho\sigma}$$

or

$$(20') \qquad (\phi_\rho,\Phi_\sigma)_r = \delta_{\rho\sigma}$$

in terms of the inner product defined above. (21) may be written as $a_\rho=(\theta,\Phi_\rho)_r$. In these equations the characters $\Phi_\rho$ are not used fully. For the $\Phi_\rho$ are defined not only for $p$-regular elements, but for all elements of $G$. Indeed (15') may be generalized to the relation

$$(22) \qquad \sum_{\rho=1}^{\ell} \phi_\rho(G_\alpha)\overline{\Phi}_\rho(G_\beta) = c(G_\alpha)\delta_{\alpha\beta}, \qquad K_\alpha\ p\text{-regular},$$

where $K_\beta$ may be $p$-singular. This we obtain directly from the orthogonality relation I, (18') by (5) and (6). For $K_\beta$ $p$-singular the right hand side is always 0. Since det $\phi\neq 0$ we have then $\Phi_\rho(G_\beta)=0$ for all $\rho$. For $p$-regular $K_\beta$, we have

$$\begin{pmatrix} \overline{\Phi}_1(G_\beta) \\ \vdots \\ \overline{\Phi}_\ell(G_\beta) \end{pmatrix} = \phi'^{-1} \begin{pmatrix} 0 \\ \vdots \\ c(G_\alpha) \\ \vdots \\ 0 \end{pmatrix}.$$

Since det $\phi\not\equiv 0 \pmod p$, this implies $\nu(\Phi_\rho(G_\beta))\geqq\nu(c(G_\beta))$, $\rho=1,\cdots,\ell$.

PROPOSITION 5. *For any $p$-singular element $G\in G$, we have*

$$(23) \qquad \Phi_\rho(G) = 0, \qquad G\ p\text{-singular};\ \rho = 1,\cdots,\ \ell.$$

*Furthermore,*

(24) $$\nu(\Phi_\rho(G)) \geqq \nu(c(G)) \qquad \rho = 1, \cdots, \ell$$

*for any element G of* $\mathfrak{G}$.

Setting $G=1$, we have in particular $\nu(\Phi_\rho(1)) \geqq \nu(c(1)) = \nu(g) = a$. Thus

PROPOSITION 6. *The degree* $\Phi_\rho(1)$ *of the character* $\Phi_\rho$ *is divisible by the p-component* $p^a$ *of g.*

§7. The $p$-rank of the matrix $D$ of decomposition numbers

The matrix $D=(d_{i\rho})$ of decomposition numbers is a $(k\times\ell)$-matrix and therefore its $p$-rank is at most equal to $\ell$; its rank is exactly $\ell$, as we see from (9) and (17). Now we wish to prove

PROPOSITION 7. *The p-rank D is equal to* $\ell$.

PROOF. It is sufficient to prove that the $p$-rank of the matrix $X_r = D\phi$ is equal to $\ell$. Suppose that this is less than $\ell$. Then there exist $\ell$ elements $\mu_\alpha$ in $\mathfrak{o}$, not all in $\mathfrak{p}$, such that

$$\sum_{K_\alpha \text{ } p\text{-regular}} \mu_\alpha \chi_i(G_\alpha) \equiv 0 \qquad (\text{mod } \mathfrak{p})$$

for all $\chi_i$. For any $\mathfrak{o}$-linear combination $\theta$ of $\chi_i$, we also have

(25) $$\sum_{K_\alpha \text{ } p\text{-regular}} \mu_\alpha \theta(G_\alpha) \equiv 0 \qquad (\text{mod } \mathfrak{p}).$$

Now the following argument is a special case of one which we gave in I, §3, Lemma 3. Let $\beta$ be an index with $\mu_\beta \not\equiv 0$ (mod $\mathfrak{p}$) and let $\mathfrak{B}=\{G_\beta\}$ be the cyclic group generated by $G_\beta$. $\mathfrak{B}$ has order $b$ prime to $p$. Let $\mathfrak{Q}$ be a Sylow $p$-subgroup of the centralizer

$C(G_\beta)$. The subgroup of $G$ generated by $G_\beta$ and $\mathcal{Q}$ is the direct product $H=\mathcal{B}\times\mathcal{Q}$. We define a class function $\theta$ of $H$ by setting

$$\theta = \sum \bar{\zeta}_j(G_\beta)\zeta_j,$$

$\zeta_j$ ranging over the irreducible characters of $\mathcal{B}$. More precisely,

$$\theta(G_\beta^n Q) = \sum_{\zeta_j} \bar{\zeta}_j(G_\beta)\zeta_j(G_\beta^n), \qquad Q \in \mathcal{Q}.$$

The last sum is $b$ or 0 according as $n\equiv 1$ or $n\not\equiv 1 \pmod b$. Thus

$$\theta(H) = \begin{cases} b & \text{if } H \in G_\beta\mathcal{Q} \\ 0 & \text{otherwise} \end{cases}$$

$\theta$ induces a class function $\theta^G=\Theta$ of $G$ by

$$\Theta(G) = \frac{1}{bq} \sum_{X\in G} \theta(XGX^{-1}),$$

where $q$ is the order of $\mathcal{Q}$, and $\theta(G)=0$ when $G\notin H$ (see I,§2). We have

$$\Theta(G_\alpha) = \begin{cases} 0 & \text{if } \alpha \neq \beta \\ \dfrac{c(G_\beta)b}{bq} = \dfrac{c(G_\beta)}{q} \not\equiv 0 \pmod p & \text{if } \alpha = \beta. \end{cases}$$

If we express the class function $\Theta$ as a linear combination of $\chi_i$, the coefficients are all in $\mathfrak{o}$ by the relation I, (27). Hence (25) must hold for this $\Theta$. But this is a contradiction, since the sum in (25) reduces then to a single term $\dfrac{\mu_\beta\, c(G_\beta)}{q}\not\equiv 0$ (mod $p$), as we have seen. This contradiction shows that the

$p$-rank of $X_r$, and hence that of $D$ is equal to $\ell$. (Actually we have proved that the $p$-rank of $X_r$ is not smaller than $\ell_0$. Since $X_r=D\phi$ and $\phi$ is an $(\ell\times\ell_0)$-matrix, this implies $\ell\geqq\ell_0$. Together with inequality $\ell\leqq\ell_0$ obtained in §4, we have another proof that $\ell=\ell_0$. We also obtain det $\phi\not\equiv 0 \pmod p$. Thus the above is an alternative approach to Proposition 4 and relation (16). The proof in [2] is along these lines.)

## §8. Blocks

In the center $Z^*=Z(G,\Omega^*)$ of $\Gamma^*=\Gamma(G,\Omega^*)$ we decompose the unit element 1 into a sum of mutually orthogonal primitive idempotents:

$$1 = \eta_1^* + \cdots + \eta_t^*. \tag{26}$$

Such a decomposition is unique (cf. I,§1). Then

$$\Gamma^* = \eta_1^*\Gamma^* + \cdots + \eta_t^*\Gamma^*, \tag{27}$$

$$Z^* = \eta_1^*Z^* + \cdots + \eta_t^*Z^* \tag{28}$$

are the unique decompositions of $\Gamma^*$, $Z^*$ respectively into a direct sum of mutually orthogonal indecomposable ideals. As indecomposable commutative algebras, the $\eta_\tau^*Z^*$ are primary and indeed

$$\eta_\tau^*Z^*/\mathrm{Rad}(\eta_\tau^*Z^*) \simeq \Omega^*$$

(cf. I,§1). If $\psi_\tau$ is the mapping $Z^*\to\eta_\tau^*Z^*\to(\eta_\tau^*Z^*/\mathrm{Rad}(\eta_\tau^*Z^*))=\Omega^*$, then for $\tau=1,\cdots,t$, we obtain $t$ linear characters $\psi_\tau$ of $Z^*$, and

$$\psi_\tau(\eta_\sigma^*) = \delta_{\tau\sigma}. \tag{29}$$

These are the totality of linear characters of $Z^*$.

To each irreducible character $\chi_i$ of $G$ there is associated an algebra homomorphism $\omega_i$ of $Z(G,\mathfrak{o})$ into $\mathfrak{o}$ (§1). $\omega_i$ induces a linear character $\omega_i^*$: $Z^*=Z(G,\mathfrak{o})/\mathfrak{p}Z(G,\mathfrak{o})\to\mathfrak{o}/\mathfrak{p}=\Omega^*$ of $Z^*$. Hence

$$\omega_i^* = \psi_\tau \tag{30}$$

for some $\tau$, and

$$\chi_i^*(\eta_\sigma^*) = \omega_i^*(\eta_\sigma^*)I = \delta_{\tau\sigma}I. \tag{31}$$

We distribute the $k$ irreducible characters $\chi_i$ into $t$ <u>blocks</u> $B_\tau$ by setting

$$B_\tau = \{\chi_i \mid \omega_i^* = \psi_\tau\}.$$

That $\chi_i$ belongs to the block $B_\tau$ is characterized by (31). It is also characterized either by

$$X_i^*(\eta_\tau^*) = I \tag{32}$$

or by

$$X_i^*(\eta_\sigma^*) = 0 \qquad \text{for all } \sigma \neq \tau. \tag{33}$$

Two irreducible characters $\chi_i$, $\chi_j$ belong to the same block if and only if $\omega_i^*=\omega_j^*$, *i.e.* if and only if

$$\frac{g}{c(G_\alpha)}\frac{\chi_i(G_\alpha)}{x_i} \equiv \frac{g}{c(G_\alpha)}\frac{\chi_j(G_\alpha)}{x_j} \qquad (\text{mod } \mathfrak{p}) \tag{34}$$

for all classes $K_\alpha$ in $G$.

If $F_\rho$ is an irreducible modular constituent of $X_i^*$, then by (31),

$$(35) \qquad F_\rho(\eta_\sigma^*) = \delta_{\tau\sigma} I.$$

We will also say that an irreducible modular representation $F_\rho$ and its character $\psi_\rho$ belong to a block $B_\tau$, in symbols $F_\rho \in B_\tau$, $\phi_\rho \in B_\tau$, when (35) holds. Each $F_\rho$ appears in at least one $X_i$, and thus each $\phi_\rho$ belongs to one and only one block. Thus the $\ell$ irreducible modular characters $\phi_\rho$ are distributed into $t$ blocks $B_\tau$. Again, that $\phi_\rho$ belongs to $B_\tau$ is characterized by (35). It is also characterized either by

$$(36) \qquad F_\rho(\eta_\tau^*) = I$$

or by

$$(37) \qquad F_\rho(\eta_\sigma^*) = 0 \qquad \text{for all } \sigma \neq \tau.$$

With the distribution of irreducible ordinary and modular characters into blocks, we have

$$\chi_i \in B_\tau \Longrightarrow \chi_i(R) = \sum_{\phi_\rho \in B_\tau} d_{i\rho}\phi_\rho(R), \ R \ p\text{-regular},$$

$$\phi_\rho \in B_\tau \Longrightarrow \Phi_\rho(G) = \sum_{\chi_i \in B_\tau} d_{i\rho}\chi_i(G), \ G \in \mathcal{G}.$$

For if $\chi_i \in B_\tau$, $\phi_\rho \in B_\sigma$ and $\tau \neq \sigma$, then $X_i^*(\eta_\tau^*) = I$, $F_\rho(\eta_\tau^*) = 0$, and evidently $F_\rho$ is not a constituent of $X_i^*$, so that $d_{i\rho} = 0$. The matrix $D$ breaks up then into $t$ parts, as does $C$.

$$(38) \qquad D = \begin{pmatrix} D_1 & & 0 \\ & \ddots & \\ 0 & & D_t \end{pmatrix} \qquad C = \begin{pmatrix} C_1 & & 0 \\ & \ddots & \\ 0 & & C_t \end{pmatrix}$$

$$D_\tau' D_\tau = C_\tau.$$

If $k_\tau$, $\ell_\tau$ denote the number respectively of ordinary and modular characters in a block $B_\tau$, then $D_\tau$ is a $(k_\tau \times \ell_\tau)$-matrix, and $C_\tau$ is a square matrix of degree $\ell_\tau$. Since the $p$-rank of $D$ has been seen to be $\ell$ and $\ell = \sum_{t=1}^{t} \ell_\tau$, we see that the $p$-rank of each $D_\tau$ is $\ell_\tau$.

Each $\ell_\tau$ is at least one, *i.e.* every block $B_\tau$ contains at least one modular character $\phi_\rho$. For if not, the idempotent $\eta^*_\tau$ would be represented in every $F_\rho$ by 0 (cf. (37)), which is a contradiction. It follows then, either by the remark at the end of §4 or by (17) and (38), that every block $B_\tau$ contains at least one ordinary irreducible character $\chi_i$. (This can be seen directly by considering the regular representation and (33)). In fact, since the $p$-rank of $D_\tau$ is $\ell_\tau$,

$$k_\tau \geqq \ell_\tau \geqq 1 \tag{39}$$

for every $\tau=1,\cdots,t$. Since $\ell_\tau \neq 0$ and det $C \neq 0$, we also have det $C_\tau \neq 0$ for every $\tau$.

## §9. Idempotents belonging to blocks

The $t$ idempotents $\eta^*_\tau$ in $Z^*=Z(G,\Omega^*)$ studied in the preceding section are in 1-1 correspondence with the $t$ blocks $B_\tau$. We now turn to $Z(G,\Omega)$, and construct there (in fact in $Z(G,o)$) $t$ idempotents in correspondence with the $t$ blocks. For this purpose, let $\varepsilon_1,\cdots,\varepsilon_k$ be the $k$ mutually orthogonal and primitive idempotents in $Z(G,\Omega)$ with the sum $1=\sum_{i=1}^{k}\varepsilon_i$, these $\varepsilon_i$ being in 1-1 correspondence with the $k$ irreducible characters $\chi_1, \cdots, \chi_k$. For each block $B_\tau$, set

$$\eta_\tau = \sum_{\chi_i \in B_\tau} \varepsilon_i. \tag{40}$$

The $t$ elements $\eta_1, \cdots, \eta_t$ are evidently mutually orthogonal idempotents in $Z(G,\Omega)$, and have the sum $\sum_{\tau=1}^{t} \eta_\tau = 1$. From (21) in I, §2, we see that

$$\omega_i(\eta_\tau) = \begin{cases} 1 & \text{if } \chi_i \in B_\tau \\ 0 & \text{if } \chi_i \notin B_\tau. \end{cases} \tag{41}$$

We want to prove that each $\eta_\tau$ belongs to $Z(G,\mathfrak{o})$ and that its residue class modulo $pZ(G,\mathfrak{o})$ is the idempotent $\eta_\tau^*$. One method of proving this is to show the existence of mutually orthogonal idempotent representations of 1 in $Z(G,\mathfrak{o})$, and to show that they satisfy the same relations as (41). This will then show that they coincide with the $\eta_\tau$.[1] However we will follow the more explicit way as given in paper [32] of Osima; the idempotents $\eta_\tau$ were effectively introduced in this paper, so that we will call them Osima's idempotents.[2] Now the idempotents $\varepsilon_i$ are explicitly given in I, (20). Hence the idempotents $\eta_\tau$ in (40) are given by

---

1) This method is used in the lectures at Tokyo University. An account can be found in the summary of K. Sekino in "Sugaku" (Mathematics), Vol. 11 (1960), page 229.

2) These were also introduced independently by H. Nagao.

(42) $$\eta_\tau = \sum_{\alpha=1}^{k} b_{\tau\alpha} K_\alpha, \text{ where } b_{\tau\alpha} = \frac{1}{g} \sum_{\chi_i \in B_\tau} x_i \overline{\chi}_i(G_\alpha).$$

PROPOSITION 8. *Each* $\eta_\tau$ *belongs to* $Z(G, \mathfrak{o})$ *and its residue class module* $pZ(G, \mathfrak{o})$ *is the idempotent* $\eta_\tau^*$ *in (26).*

PROOF. For any block $B_\tau$ and any class $K_\alpha$, we have

(43) $$\begin{aligned} b_{\tau\alpha} &= \sum_{\chi_i \in B} \frac{x_i}{g} \overline{\chi}_i(G_\alpha) = \frac{1}{g} \sum_{\chi_i \in B_\tau} \chi_i(1)\overline{\chi}_i(G_\alpha) \\ &= \frac{1}{g} \sum_{\chi_i \in B_\tau} \Big( \sum_{\phi_\rho \in B_\tau} d_{i\rho}\phi_\rho(1)\overline{\chi}_i(G_\alpha)\Big) \\ &= \frac{1}{g} \sum_{\phi_\rho \in B_\tau} \Big( \sum_{\chi_i \in B_\tau} d_{i\rho}\overline{\chi}_i(G_\alpha)\Big)\phi_\rho(1) \\ &= \frac{1}{g} \sum_{\phi_\rho \in B_\tau} \phi_\rho(1)\overline{\Phi}_\rho(G_\alpha). \end{aligned}$$

If the class $K_\alpha$ is $p$-singular, then $\Phi_\rho(G_\alpha)=0$ for all $\rho$ by Proposition 5, and hence $b_{\tau\alpha}=0$. For a $p$-regular class $K_\alpha$, we have

$$\begin{aligned} b_{\tau\alpha} &= \frac{1}{g} \sum_{\chi_i \in B_\tau} \chi_i(1)\overline{\chi}_i(G_\alpha) \\ &= \frac{1}{g} \sum_{\chi_i \in B_\tau} \chi_i(1) \sum_{\phi_\rho \in B_\tau} d_{i\rho}\overline{\phi}_\rho(G_\alpha) \\ &= \frac{1}{g} \sum_{\phi_\rho \in B_\tau} \Phi_\rho(1)\overline{\phi}_\rho(G_\alpha). \end{aligned}$$

Here $\nu(\Phi_\rho(1)) \geqq \nu(g)=a$ by Proposition 6, and hence $b_{\tau\alpha} \in \mathfrak{o}$. This proves $\eta_\tau \in Z(G, \mathfrak{o})$.

Next we have $\omega_i(\eta_\tau)=\sum_{\chi_j\epsilon B}\omega_i(\varepsilon_j)$, and this is 1 or 0 according as $\chi_i \epsilon B_\tau$ or not by I, (23). Hence if we denote the residue class of $\eta_\tau$ module $pZ(G,\mathfrak{o})$ by $[\eta_\tau]^*$, then

(44)
$$\omega_i^*([\eta_\tau]^*) = \begin{cases} 1 & \text{if } \chi_i \in B_\tau \\ 0 & \text{otherwise.} \end{cases}$$

In particular $[\eta_\tau]^* \neq 0$ for all $\tau$. Furthermore, since the $[\eta_\tau]^*$ are evidently mutually orthogonal idempotents in $Z(G,\mathfrak{o})/pZ(G,\mathfrak{o})$ $=Z(G,\Omega^*)$, the uniqueness of the decomposition of 1 into primitive idempotents in a commutative algebra implies that the totality of the $[\eta_\tau]^*$ coincides with that of the $\eta_\tau^*$. Relation (44) implies furthermore that

$$[\eta_\tau]^* = \eta_\tau^*, \qquad \tau = 1,\cdots, t.$$

Incidentally, we have proved that

$$\eta_\tau = \sum_{K_\alpha \ p\text{-regular}} b_{\tau\alpha}K_\alpha, \qquad b_{\tau\alpha} \in \mathfrak{o}.$$

We have therefore $\eta_\tau^*=\sum_{K_\alpha \ p\text{-regular}} b_{\tau\alpha}^*K_\alpha$, where $b_{\tau\alpha}^*$ denotes the residue class of $b_{\tau\alpha}$ (mod $p$). This last equation can be refined to

(45)
$$\eta_\tau^* = \sum_{\substack{K_\alpha \ p\text{-regular} \\ \nu(c(G_\alpha)) \leqq d_\tau}} b_{\tau\alpha}^*K_\alpha,$$

where

(46)
$$d_\tau = \operatorname*{Max}_{\phi_\rho \in B_\tau} \nu\left(\frac{g}{f_\rho}\right).$$

For by (43) we have

$$\nu(b_{\tau\alpha}) = \nu\Big(\frac{1}{g}\sum_{\phi_\rho\in B_\tau}\phi_\rho(1)\Phi_\rho(G_\alpha)\Big)$$

$$\geqq \operatorname*{Min}_{\phi_\rho\in B_\tau}\Big(\nu\Big(\frac{f_\rho}{g}\Big)+\nu(\Phi_\rho(G_\alpha))\Big) \geqq \operatorname*{Min}_{\phi_\rho\in B_\tau}\ \nu(\Phi_\rho(G_\alpha)) - d_\tau$$

and this is in turn $\geqq\nu(c(G_\alpha))-d_\tau$ by Proposition 5. Hence if $\nu(c(G_\alpha))>d_\tau$, then $\nu(b_{\tau\alpha})>0$, or $b^*_{\tau\alpha}=0$, which proves (45).

## §10. Defect of a block

The number $d_\tau$ defined in (46) is called the <u>defect</u> of the block $B_\tau$. Thus

$$d_\tau = \operatorname*{Max}_{\phi_\rho\in B_\tau}(a-\nu(f_\rho)) = a - \operatorname*{Min}_{\phi_\rho\in B_\tau}\nu(f_\rho).$$

In other words,

$$\begin{aligned}\nu(f_\rho) &\geqq a - d_\tau \qquad \text{for all } \phi_\rho \in B_\tau,\\ &= a - d_\tau \qquad \text{for some } \phi_\rho \in B_\tau.\end{aligned}$$

As

(47) $$x_i = \sum_{\phi_\rho\in B_\tau} d_{i\rho}f_\rho \qquad \text{for } \chi_i \in B_\tau,$$

we have clearly $d_\tau \geqq \operatorname*{Max}_{\chi_i\in B_\tau}\nu\big(\frac{g}{x_i}\big)$. Actually the equality holds, so that the defect $d_\tau$ may also be defined by means of the degrees of the ordinary irreducible characters $\chi_i$ as well as by means of the degrees of the irreducible modular characters $\phi_\rho$ as in (46). Namely, we have

PROPOSITION 10. *We have*

(48) $$d_\tau = \operatorname*{Max}_{\chi_i \in B_\tau} \nu\left(\frac{g}{x_i}\right).$$

PROOF. As we have seen in §8, the $p$-rank of $D_\tau = (d_{i\rho})_{\chi_i, \phi_\rho \in B_\tau}$ is equal to the number $\ell_\tau$ of irreducible modular characters $\phi_\rho$ in $B_\tau$. The relation (47) then implies $\operatorname*{Min}_{\chi_i \in B_\tau} \nu(x_i) = \operatorname*{Min}_{\phi_\rho \in B_\tau} \nu(f_\rho)$, and this proves (48).

We now define the <u>defect</u> $d_G$ of an element $G \in G$ to be the non-negative integer

(49) $$d_G = \nu(c(G)).$$

The defect of a conjugate class $K_\alpha$ of $G$ is defined to be the defect of a representative $G_\alpha$; this is evidently independent of the choice of representative. With this terminology we can say that the sum in the right hand side of (45) ranges over $p$-regular class with defect at most equal to $d$.

PROPOSITION 11. *An irreducible character $\chi_i$ belongs to a block of defect $d$ if and only if $\omega_i(K_\alpha) \equiv 0$ (mod $p$) for all classes $K_\alpha$ of defect $<d$, but not for all $p$-regular classes $K_\alpha$ of defect $d$.*

PROOF. Let $B_\tau$ be the block of $\chi_i$ and set $\nu(x_i) = \nu(\chi_i(1)) = a - d_\tau + h_i$, where $h_i \geqq 0$. Since $\omega_i(K_\alpha) = \frac{g}{c(G_\alpha)} \frac{\chi_i(G_\alpha)}{x_i}$, we have

$$\begin{aligned} \nu(\omega_i(K_\alpha)) &= a - \nu(c(G_\alpha)) + \nu(\chi_i(G_\alpha)) - a + d_\tau - h_i \\ &\geqq d_\tau - \nu(c(G_\alpha)) - h_i. \end{aligned}$$

There exists an irreducible character $\chi_j$ in $B_\tau$ with $h_j = 0$; for it we have similarly

$$\nu(\omega_j(K_\alpha)) \geq d_\tau - \nu(c(G_\alpha)) - h_j = d_\tau - \nu(c(G_\alpha)).$$

If the class $K_\alpha$ has defect $\nu(c(G_\alpha))<d_\tau$, we have $\nu(\omega_j(K_\alpha))>0$, or $\omega_j(K_\alpha)\equiv 0 \pmod p$. Since $\omega_i(K_\alpha)\equiv\omega_j(K_\alpha) \pmod p$, we have $\omega_i(K_\alpha)\equiv 0 \pmod p$ too. Together with (31) and (45), this yields

$$1 = \sum_{\substack{K_\alpha \ p\text{-regular} \\ d_{G_\alpha}=d_\tau}} b^*_{\tau\alpha}\omega^*_i(K_\alpha).$$

Hence there exists at least one $p$-regular class $K_\alpha$ with defect equal to $d_\tau$ such that $\omega^*_i(K_\alpha)\neq 0$. The defect $d_\tau$ of the block $B_\tau$ is thus the smallest integer $d$ such that $\omega_i(K_\alpha)\not\equiv 0 \pmod p$ for some $p$-regular class $K_\alpha$ of defect $d$. The above relation and (45) also show that $d_\tau$ is the largest of the defects $\nu(c(G_\alpha))$ of the $p$-regular classes $K_\alpha$ with $b^*_{\tau\alpha}\neq 0$.

PROPOSITION 12. *Let $\chi_i$ and $\chi_j$ be two irreducible characters belonging to blocks of the same defect $d$. Then they belong to the same block if and only if $\omega_i(K_\alpha)\equiv\omega_j(K_\alpha)$ (mod $p$) for all $p$-regular classes $K_\alpha$ of defect $d$.*

PROOF. By (45) and the above proposition we have

$$\omega^*_i(\eta^*_\tau) = \sum_{\substack{K_\alpha \ p\text{-regular} \\ \text{class of defect } d}} b^*_{\tau\alpha}\omega^*_i(K_\alpha) \tag{50}$$

for every block $B_\tau$ of defect $d_\tau=d$. For such a block $B_\tau$ we also have

$$\omega^*_j(\eta^*_\tau) = \sum_{\substack{K_\alpha \ p\text{-regular} \\ \text{class of defect } d}} b^*_{\tau\alpha}\omega^*_j(K_\alpha).$$

So, if $\omega_i(K_\alpha)\equiv\omega_j(K_\alpha)$ (mod $p$) for all $p$-regular classes $K_\alpha$ of defect $d$, then $\omega_i^*(\eta_\tau^*)=\omega_j^*(\eta_\tau^*)$ for every block $B_\tau$ of defect $d$. The last equation holds trivially for every block $B_\tau$ of defect $\neq d$, since both sides are 0. Hence $\omega_i^*(\eta_\tau^*)=\omega_j^*(\eta_\tau^*)$ for every block $B_\tau$, and $\chi_i$ and $\chi_j$ belong to the same block. The coverse is obvious.

The proofs of Propositions 11, 12 in these notes are due to Osima [32]. The author's own proofs are in [20]. Each has its advantage.

## §11. The determinant of the matrix $C$ of Cartan invariants

$C$ is a matrix with rational, integral coefficients. Its determinant is therefore a rational integer, and as was proved, non-zero. Since $C=D'D$, the determinant is in fact positive. We prove first

PROPOSITION 13. *The determinant of $C$ is a power of $p$.*
We start with

LEMMA 1. *Let $g=p^a g'$, where $(g',p)=1$. Let $\phi$ be a modular character of $G$ (with respect to the prime $p$), and set*

$$\theta(G) = \begin{cases} p^a\phi(G) & \text{if } G \text{ is } p\text{-regular} \\ 0 & \text{if } G \text{ is } p\text{-singular}. \end{cases}$$

*Then $\theta\in X_Z(G)$ (in the notation of* I, §3*), i.e. $\theta$ is a linear combination of ordinary irreducible characters of $G$ with rational, integral coefficients.*

PROOF. By I, §3, Proposition 10' for the case $K=\Omega$, it is sufficient to show that for every elementary subgroup $H$ of $G$, the restriction $\theta|H$ belongs to $X_Z(H)$. $H$ is the direct product of a $q$-group and a cyclic group, where $q$ is a prime which may or may not be $p$. In any case $H$ is the direct product of a $p$-group $P$ and a group $B$ whose order is prime to $p$:

$$H = P \times B.$$

Now if $H \in H$, and if $H=PB$ with $P \in P$, $B \in B$, we set

$$\psi(H)=\rho(P)\phi(B)$$

where $\rho$ is the character of the ordinary regular representation of $P$. Since the restriction of $\phi$ to $B$ may be regarded as an ordinary character of $B$, $\psi$ is an ordinary character of $H$. If we set $(P:1)=p^s$, we have

$$\psi(H) = \begin{cases} p^s\phi(H) & \text{if } P = 1 \\ 0 & \text{if } P \neq 1. \end{cases}$$

Hence $\theta|H$ is just $p^{a-s}\psi$, and $\theta|H \in X_Z(H)$.

We now prove Proposition 13. Let $\phi_\lambda$, $\lambda=1,\cdots,\ell$, be the irreducible modular characters of $G$ (for the prime $p$). For each $\lambda=1,\cdots,\ell$, set

$$\theta_\lambda(G) = \begin{cases} p^a\phi_\lambda(G) & \text{if } G \text{ is } p\text{-regular} \\ 0 & \text{if } G \text{ is } p\text{-singular}. \end{cases}$$

By our lemma we have

$$\theta_\lambda = \sum_{i=1}^{k} a_{i\lambda}\chi_i,$$

where the $a_{i\lambda} \in Z$, and the $\chi_i$ are the ordinary irreducible characters of $G$. Here

$$a_{i\lambda} = (\theta_\lambda, \chi_i) = \frac{1}{g}\sum_G \theta_\lambda(G)\overline{\chi}_i(G) = \frac{1}{g}\sum_{G\ p\text{-regular}} \theta_\lambda(G)\overline{\chi}_i(G)$$

$$= \frac{1}{g}\sum_{G\ p\text{-regular}} p^a\phi_\lambda(G)\sum_{\mu=1}^{\ell} d_{i\mu}\overline{\Phi}_\mu(G)$$

$$= p^a\sum_{\mu=1}^{\ell} d_{i\mu}\sum_{G\ p\text{-regular}} \phi_\lambda(G)\,\frac{1}{g}\,\overline{\Phi}_\mu(G)$$

$$= p^a\sum_{\mu=1}^{\ell} d_{i\mu}\sum_{K_\alpha\ p\text{-regular}} \phi_\lambda(G_\alpha)\,\frac{1}{c(G_\alpha)}\,\overline{\Phi}_\mu(G_\alpha)$$

where the $d_{i\mu}$ are the decomposition numbers, and $G_\alpha$ are representatives of the $p$-regular conjugate classes $K_\alpha$ of $G$. Since $\phi N_r^{-1}\overline{\Phi}'=C^{-1}$ by (18), we have

$$a_{i\lambda} = p^a\sum_{\mu=1}^{\ell} d_{i\mu}\gamma_{\mu\lambda}$$

where we set $C^{-1}=(\gamma_{\mu\lambda})$. If we denote the matrix $(a_{i\lambda})$ by $A$, then we can rewrite the above as

$$A = p^a DC^{-1}.$$

Since $C=D'D$ and $C'=C$, we have furthermore

$$CA'A = p^{2a}CC^{-1}D'DC^{-1} = p^{2a}I,$$

and hence $\det C\cdot\det A'A=p^{2a\ell}$. Since both $C$ and $A'A$ are matrices with coefficients in $Z$, $\det C$ is thus a power of $p$.

The exact value of the determinant of $C$ can now be readily obtained. The determinant of the matrix $\phi$ in (15) is a unit in the domain $\mathfrak{o}$ of $p$-integers (*i.e.* the domain of integers for $\nu$), and the same is true for the determinant of $\overline{\Phi}$, since $\overline{\Phi}$ is obtained from $\phi$ by a permutation of the columns. Hence relation (15) and the form (11) of $N_r$ show that the $p$-component of $\det C$ is that of $c(G_1)\cdots c(G_\ell)$. But the $p$-component of a rational integer coincides with its $p$-component. This together with Proposition 13 implies

PROPOSITION 14. *The determinant of the matrix $C$ of Cartan invariants is the highest power of $p$ dividing the product $c(G_1) \cdots c(G_\ell)$.*

Propositions 13 and 14 were first proved in [4] by different methods. The present proofs, depending on I, §3, Proposition 10', were given in [18].

## §12. The elementary divisors of $C$ and $C_\tau$

The above considerations give us not only the determinant of $C$, but the elementary divisors of $C$ as well. Indeed, (15) and (11) imply that the elementary divisors of $C$, as a matrix in $o$, are up to order the $p$-components of $c(G_1), \cdots, c(G_\ell)$. This implies that the $p$-components of the elementary divisors of $C$, as a matrix with rational, integral coefficients, are up to order, the $p$-components of $c(G_1), \cdots, c(G_\ell)$. Together with Proposition 13 this yields.

PROPOSITION 15. *The elementary divisors of $C$, as a matrix in the domain of rational integers, are up to order the highest powers of $p$ dividing the numbers $c(G_1), \cdots, c(G_\ell)$.*

Now according to (38), the matrix $C$ breaks up into $t$ parts $C_\tau$ corresponding to the $t$ blocks $B_\tau$. The $\ell$ elementary divisors of $C$ are distributed accordingly into $t$ sets.

PROPOSITION 16. *Assume a fixed enumeration of the $\ell$*

*irreducible modular characters* $\phi_\rho$, $\rho=1,\cdots,\ell$. *For each block* $B_\tau$ *let* $S_\tau$ *be the set of indices* $\rho$ *with* $\phi_\rho\in B_\tau$. *We can then enumerate the* $\ell$ *p-regular conjugate classes* $K_\sigma$, *such that for each block* $B_\tau$, *we have*

$$(51)\qquad \det(\phi_\rho(G_\sigma))_{\rho,\sigma\in S_\tau} \not\equiv 0 \qquad (\text{mod } p),$$

*where* $G_\sigma$ *is a representative of* $K_\sigma$. *The elementary divisors of* $C$ *belonging to* $B_\tau$ *(i.e. the elementary divisors of* $C_\tau$*) are then up to order the p-components of* $c(G_\sigma)$, $\sigma\in S_\tau$.

PROOF. For any enumeration $K_\sigma$, $\sigma=1,\cdots,\ell$, of the $p$-regular classes we have $\det\phi=\det(\phi_\rho(G_\sigma))_{\rho,\sigma=1,\cdots,\ell}\not\equiv 0$ (mod $p$) by (16). Hence by Laplace's theorem,

$$\det\phi = \sum_T \pm\, \Delta_1^{(T)}\Delta_2^{(T)}\,\cdots\,\Delta_t^{(T)}.$$

Here $T$ runs over all distinct partitions of $1,\cdots,\ell$ into $t$ sets $T_\tau$, $\tau=1,\cdots,t$, each $T_\tau$ consisting of $\ell_\tau$ members; $\Delta_\tau^{(T)}$ denotes the subdeterminant $\det(\phi_\rho(G_\sigma))_{\rho\in S_\tau,\sigma\in T_\tau}$. Hence there must exist at least one partition $T$ such that

$$\Delta_1^{(T)}\Delta_2^{(T)}\,\cdots\,\Delta_t^{(T)} \not\equiv 0 \qquad (\text{mod } p).$$

This implies however that $\Delta_\tau^{(T)}\not\equiv 0$ (mod $p$), or $\det(\phi_\rho(G_\alpha))_{\rho\in S_\tau,\sigma\in T_\tau}$ $\not\equiv 0$ (mod $p$) for each $\tau$. If we enumerate the $K_\alpha$ so that $T_\tau$ coincides with $S_\tau$ for each $\tau$, which is certainly possible, we then have (51) for each $\tau$, which proves the first half of the proposition.

To prove the second half, fix a block $B_\tau$, and let $p^{e_\rho}$ be the elementary divisors of $C_\tau$, where the indices $\rho$ run through $S_\tau$.

Let $H$ be the diagonal matrix having the entries $p^{e_1}, \cdots, p^{e_{\ell_\tau}}$ on its main diagonal, and let $U$, $V$ be unimodular matrices of degree $\ell_\tau$ such that

(52) $$UC_\tau V^{-1} = H.$$

We may index the rows and columns of $U$, $V$ by the indices of $S_\tau$. Thus set $U=(u_{\rho\sigma})_{\rho,\sigma\in S_\tau}$, $V=(v_{\rho\sigma})_{\rho,\sigma\in S_\tau}$. For $\rho\in S_\tau$, set

$$\tilde{\Phi}_\rho = \sum_{\sigma\in S_\tau} u_{\rho\sigma}\Phi_\sigma, \quad \tilde{\phi}_\rho = \sum_{\sigma\in S_\tau} v_{\rho\sigma}\phi_\sigma,$$

where the $\Phi_\sigma$ are the characters defined in (6). Then (7) and (52) imply

$$\tilde{\Phi}_\rho(R) = p^{e_\rho}\tilde{\phi}_\rho(R), \qquad \rho \in S_\tau,$$

for any $p$-regular element $R$. It follows from Proposition 5 that

(53) $$e_\rho + \nu(\tilde{\phi}_\rho(R)) \geq \nu(c(R)), \qquad \rho \in S_\tau,$$

for $p$-regular $R$. However, we have

$$\det(\tilde{\phi}_\rho(G_\sigma))_{\rho,\sigma\in S_\tau} = \det V \det(\phi_\rho(G_\sigma))_{\rho,\sigma\in S_\tau},$$

and since $V$ is unimodular, we have by (51)

$$\det(\tilde{\phi}_\rho(G_\sigma))_{\rho,\sigma\in S_\tau} \not\equiv 0 \qquad (\mathrm{mod}\ p).$$

Hence there exists a permutation $\pi_\tau$ of the $\ell_\tau$ indices in $S_\tau$ such that $\prod_{\rho\in S_\tau} \tilde{\phi}_\rho(G_{\pi_\tau(\rho)})\not\equiv 0$ (mod $p$), or $\nu(\tilde{\phi}_\rho(G_{\pi_\tau(\rho)}))=0$ for each $\rho\in S_\tau$. The inequality (53) gives then

(54) $$e_\rho \geq \nu(c(G_{\pi_\tau(\rho)})), \qquad \rho \in S_\tau.$$

We may now suppose that $\pi_\tau$ has been chosen for each $\tau$ so that (54) is the case for each $\tau$. But by Proposition 14 the sums of the left and right hand sides of (54) summed over the block indices $\tau=1,\cdots,t$ are the same. Hence the inequalities (54) must be in fact equalities, and this proves the second part of Proposition 16.

We now study the relation between the defect of a block $B_\tau$ and the elementary divisors of $C_\tau$. Let the multiplication in $Z(G,o)$ of the sums $K_\alpha$ of the elements of the conjugate classes $K_\alpha$ be given by

$$K_\alpha K_\beta = \sum_\gamma a_{\alpha\beta\gamma} K_\gamma . \tag{55}$$

Thus each coefficient $a_{\alpha\beta\gamma}$ is a non-negative integer, equal to the number of pairs $X\in K_\alpha$, $Y\in K_\beta$ such that $XY$ is a fixed element, say $G_\gamma$, of $K_\gamma$. Clearly we have $a_{\alpha\beta\gamma}=a_{\beta\alpha\gamma}$.

LEMMA 2. *If $G_\alpha$, $G_\gamma$ are representatives of $K_\alpha$, $K_\gamma$ respectively, and if $\nu(c(G_\alpha))<\nu(c(G_\gamma))$, then $a_{\alpha\beta\gamma}\equiv 0$ (mod $p$) for any $\beta$.*

PROOF. $a_{\alpha\beta\gamma}g/c(G_\gamma)$ is the number of pairs $X\in K_\alpha$, $Y\in K_\beta$ such that the product $W=XY$ lies in $K_\gamma$. This number is equal to the number of pairs $W\in K_\gamma$, $Y\in K_\beta$ with $WY^{-1}\in K_\alpha$, *i.e.* to $a_{\gamma\beta'\alpha}g/c(G_\alpha)$, where $K_{\beta'}$ is the conjugate class consisting of the inverses of the elements of $K_\beta$. Thus $a_{\alpha\beta\gamma}=a_{\gamma\beta'\alpha}c(G_\gamma)/c(G_\alpha)$ and our lemma is evident.

Now from I, (24) we deduce

$$\eta_\tau K_\alpha = \frac{1}{c(G_\alpha)} \sum_\gamma \sum_{\chi_i\in B_\tau} \chi_i(G_\alpha)\overline{\chi}_i(G_\gamma)K_\gamma . \tag{56}$$

Let $K_{\tau,\nu}$, $\nu=1,\cdots,\ell_\tau$, be the $\ell_\tau$ classes $K_\alpha$, $\alpha\in S_\tau$, associated with the block $B_\tau$ by Proposition 16, and $K_{\tau,\nu}$, $G_{\tau,\nu}$ respectively the sum of the elements, a representative of $K_{\tau,\nu}$. We thus have

$$(57) \qquad (\eta_1 K_{1,1},\cdots,\eta_\tau K_{\tau,\mu},\cdots,\eta_t K_{t,\ell_t}) = (K_{1,1},\cdots,K_{\tau,\mu},\cdots,K_{t,\ell_t})M,$$

where $M$ is the matrix

$$M = \left(\frac{1}{c(G_{\tau,\mu})}\sum_{\chi_i\in B_\tau}\chi_i(G_{\tau,\mu})\overline{\chi}_i(G_{\omega,\nu})\right)_{(\omega,\nu),(\tau,\mu)}$$

having the pairs $(\omega,\nu)$, $(\tau,\mu)$ as row and column indices respectively. The coefficients of $M$ lie in $o$, since Osima's idempotents $\eta_\tau$ are $o$-linear combinations of the $K_\alpha$. Furthermore

$$\begin{aligned}\sum_{\chi_i\in B_\tau}\chi_i(G_{\tau,\mu})\overline{\chi}_i(G_{\omega,\nu}) &= \sum_{\chi_i\in B_\tau}\sum_{\phi_\rho\in B_\tau} d_{i\rho}\phi_\rho(G_{\tau,\mu})\sum_{\phi_\sigma\in B_\tau} d_{i\sigma}\overline{\phi}_\sigma(G_{\omega,\nu})\\ &= \sum_{\phi_\rho\in B_\tau}\sum_{\phi_\sigma\in B_\tau}\phi_\rho(G_{\tau,\mu})c_{\rho\sigma}\overline{\phi}_\sigma(G_{\omega,\nu}).\end{aligned}$$

Thus

$$\det M = \frac{\det(\psi'\overline{\phi})}{\prod_{\tau,\mu} c(G_{\tau,\mu})},$$

where $\phi$ is as before the matrix of irreducible modular characters, and $\psi$ is the matrix

$$\psi = \begin{pmatrix}\psi_1 & & 0\\ & \ddots & \\ 0 & & \psi_t\end{pmatrix} \text{ with } \psi_\tau = (\phi_\sigma(G_{\tau,\mu})),\ \mu = 1,\cdots,\ \ell_\tau;\ \sigma\in S_\tau.$$

Since by Proposition 16 $\nu(\det\overline{\phi})=0$ and $\nu(\det\psi_\tau)=\nu(\det C_\tau)+\nu(\det\phi_\rho(G_{\tau,\mu}))_{\rho\in S_\tau,\mu=1,\cdots,\ell_\tau}=\nu(\prod_{\mu=1}^{\ell_\tau} c(G_{\tau,\mu}))$, we have $\nu(\det M)=0$, or $\det M\not\equiv 0 \pmod{p}$. This shows that the $\ell=\sum_\tau \ell_\tau$ elements $\eta_1^* K_{1,1}$, $\cdots,\eta_\tau^* K_{\tau,\mu},\cdots,\eta_t^* K_{t,\ell_t}$, which are the residue classes modulo $p$

of the elements of the left hand side of (57), are linearly independent over $\Omega^*=o/p$, so that each $K_{\tau,\mu}$ is a linear combination of these elements over $\Omega^*$. In particular, every $\eta_\tau^*$ is a linear combination of the $\eta_\omega^* K_{\omega,\nu}$, over $\Omega^*$. But since $\eta_\tau^{*2}=\eta_\tau^*$, in such an expression for $\eta_\tau^*$, only terms with $\omega=\tau$, *i.e.* $\eta_\tau^* K_{\tau,\nu}$, $\nu=1,\cdots,\ell_\tau$, need be considered. It follows by the above lemma that $\eta_\tau^*$ is a linear combination over $\Omega^*$ of those $K_\alpha$ such that $\nu(c(G_\alpha))\leq \nu(c(G_{\tau,\nu}))$ for some class $K_{\tau,\nu}$ associated with $B_\tau$.

We now prove

PROPOSITION 17. *If $B_\tau$ is a block of defect $d=d_\tau$, the matrix $C_\tau$ has one and only one elementary divisor $p^d$. All other elementary divisors of $C_\tau$ are smaller powers of $p$.*

PROOF. By the above result and a remark made prior to Proposition 12, there exists among the classes associated with $B_\tau$ a class $K_{\tau,\mu}$ such that $d_\tau\leq\nu(c(G_{\tau,\mu}))$. Since the $p$-rank of $D_\tau$ is $\ell_\tau$ (§§7,8), there are $\ell_\tau$ ordinary irreducible characters $\chi_{\tau,1},\cdots,\chi_{\tau,\ell_\tau}$ such that the corresponding $\ell_\tau$ rows of $D_\tau$ are linearly independent (mod $p$). Hence by our choice of $K_{\tau,1},\cdots,K_{\tau,\ell_\tau}$

$$(58)\qquad \det(\chi_{\tau,i}(G_{\tau,\nu}))_{i,\nu=1,\cdots,\ell_\tau}\not\equiv 0 \qquad (\mathrm{mod}\ p).$$

Multiply a column, say the $\nu$-th by $g/c(G_{\tau,\nu})$. Now $g\chi_{\tau,i}(G_{\tau,\nu})/c(G_{\tau,\nu})=x_{\tau,i}\omega_{\tau,i}(K_{\tau,\nu})$, where $x_{\tau,i}$ is the degree of $\chi_{\tau,i}$ and $\omega_{\tau,i}$ is the linear character of the center of the group ring corresponding to $\chi_{\tau,i}$. Since $\omega_{\tau,i}(K_{\tau,\nu})$ is integral, the determinant of the new matrix thus obtained is divisible by $p^{a-d_\tau}$. On the other hand, the exact power of $p$ dividing the determinant is by

(58) equal to $p^{\nu(g/c(G_{\tau,\nu}))}=p^{a-\nu(c(G_{\tau,\nu}))}$. Hence

(59) $$\nu(c(G_{\tau,\nu})) \leq d_\tau,$$

and this is the case for $\nu=1,\cdots,\ell_\tau$. In particular, for the index $\mu$ chosen at the beginning of the proof, we thus have

(60) $$\nu(c(G_{\tau,\mu})) = d_\tau.$$

This proves our proposition in case $\ell_\tau=1$. Assume then $\ell_\tau\geq 2$, and consider an index $\nu$ different from the index $\mu$ in (60). Multiply the $\mu$-th and $\nu$-th columns of the matrix in (58) by $g/c(G_{\tau,\mu})$ and $g/c(G_{\tau,\nu})$ respectively. The new $\mu$-th and $\nu$-th columns consists of $x_{\tau,i}\omega_{\tau,i}(K_{\tau,\mu})$ and $x_{\tau,i}\omega_{\tau,i}(K_{\tau,\nu})$ respectively. When divided by $p^{a-d_\tau}$, they become the columns $(\frac{x_{\tau,i}}{p^{a-d_\tau}}\omega_{\tau,i}(K_{\tau,\mu}))$, $(\frac{x_{\tau,i}}{p^{a-d_\tau}}\omega_{\tau,i}(K_{\tau,\nu}))$, which are congruent modulo $p$ to $(\frac{x_{\tau,i}}{p^{a-d_\tau}}\omega^*_{\tau,i}(K_{\tau,\mu}))$, $(\frac{x_{\tau,i}}{p^{a-d_\tau}}\omega^*_{\tau,i}(K_{\tau,\nu}))$, and hence proportional. It follows that the quotient of the determinant of our new matrix by $p^{2(a-d_\tau)}$ is still divisible by $p$. The exact exponent of $p$ occurring in it is, on the other hand, equal to $\nu(g/c(G_{\tau,\mu}))+\nu(g/c(G_{\tau,\nu}))=2a-\nu(c(G_{\tau,\mu}))-\nu(c(G_{\tau,\nu}))$ by (58). Hence

(61) $$\nu(c(G_{\tau,\mu})) + \nu(c(G_{\tau,\nu})) < 2d_\tau,$$

and because of (60),

(62) $$\nu(c(G_{\tau,\nu})) < d_\tau \qquad \text{for } \nu \neq \mu.$$

This proves our proposition.

Proposition 17 was first announced in [6], [10]. Our present proof is a combination of those in [20] and in Osima [32], and differs from that sketched in footnote 18) of [6].

## §13. The number of irreducible characters in a block

Consider first a block $B_\tau$ of defect $d=0$. Proposition 17 shows that the corresponding part $C_\tau$ of the matrix of Cartan invariants has only one elementary divisor, which is in fact 1. Thus $C_\tau=(1)$. Since $D_\tau$ is a matrix with non-negative rational, integral coefficients, and none of its rows consists wholly of 0's, we must have by the last relation in (38) that $D_\tau=(1)$ too. Thus a block of defect 0 consists of a single ordinary irreducible character and a single modular irreducible character. In the general case we have

PROPOSITION 18.[1] *Let $B_\tau$ be a p-block of defect d. The number k of ordinary irreducible characters $\chi_i$ in $B_\tau$ satisfies*

$$k < \tfrac{1}{4}p^{2d} + 1.$$

PROOF. Consider the matrix $A=(a_{ij})$, where

$$a_{ij} = (p^d/g) \sum_{R\ p\text{-regular}} \chi_i(R)\overline{\chi}_j(R), \qquad i,\ j = 1,\cdots,k \tag{63}$$

the summation extending over all $p$-regular elements $R$ in $G$. Let $D=D_\tau$, $C=C_\tau$ denote the matrices of decomposition numbers and Cartan invariants for $B=B_\tau$. By (5) and the orthogonality relation (18) of modular characters, we have

1) This proposition appeared in Brauer-Feit [23], and is an improvement of a weaker inequality in [13]. Readers are referred to the same paper [23] for further results in this vein.

(64) $$A = p^d D C^{-1} D'.$$

It is clear that $A$ is symmetric. Furthermore, the coefficients $a_{ij}$ of $A$ are rational integers, since the matrix $D$ has rational integral coefficients and the largest elementary divisor of $C$ is $p^d$ by Proposition 17.

By Proposition 7 there are unimodular matrices $U$, $V$ in $\mathfrak{o}$ respectively of degree $k$, $\ell$ ($\ell$ is the number $\ell_\tau$ of irreducible modular character in $B$) such that

$$UDV = \begin{pmatrix} I \\ 0 \end{pmatrix},$$

where $I$ is the unit matrix of degree $\ell$. We have

$$UAU' = p^d \begin{pmatrix} I \\ 0 \end{pmatrix} V^{-1}C^{-1}V^{-1\prime}(I,0) = p^d \begin{pmatrix} V^{-1}C^{-1}V^{-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence there exists a unimodular matrix $U_0$ in $\mathfrak{o}$ of degree $k$ such that

$$U_0AU_0' = p^d \begin{pmatrix} C^{-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

Again by Proposition 17, it follows that not all the coefficients of $A$ are divisible by $p$.

If $x_i$ denotes the degree $\chi_i(1)$ of $\chi_i$, and $\omega_i$ has its by now usual meaning, then by (63)

$$a_{ij} = \left(\frac{p^d}{g}\right)x_i \sum_{\substack{p\text{-regular} \\ \text{classes } K_\alpha}} \omega_i(K_\alpha)\overline{\chi}_j(G_\alpha),$$

or

(65) $$\left(\frac{g}{p^d}\right)(a_{ij}/x_i) = \sum_{\substack{p\text{-regular} \\ \text{classes } K_\alpha}} \omega_i(K_\alpha)\overline{\chi}_j(G_\alpha).$$

If $\chi_r$ is another ordinary irreducible character in $B=B_\tau$, then $\omega_i(K_\alpha)\equiv\omega_r(K_\alpha)$ (mod $\mathfrak{p}$) for a prime ideal divisor $\mathfrak{p}$ of $p$ in $\Omega$. (65) and the corresponding formula for $\chi_r$ yield

$$(66) \qquad (g/p^d)(a_{ij}/x_i) \equiv (g/p^d)(a_{rj}/x_r) \qquad (\text{mod } \mathfrak{p}).$$

If $\nu$ is the $\mathfrak{p}$-adic exponential valuation with $\nu(p)=1$, then $\nu(x_i)=\nu(g)-d+\lambda_i$, $\lambda_i\geq 0$. Choose $\chi_r$ so that $\lambda_r=0$, *i.e.*

$$\nu(x_r) = \nu(g) - d.$$

Then (66) implies the congruence

$$a_{ij} \equiv (x_i/x_r)a_{rj} \qquad (\text{mod } p^{1+\lambda_i})$$

in the ring of $\mathfrak{p}$-local integers. Similarly,

$$a_{jr} \equiv (x_j/x_r)a_{rr} \qquad (\text{mod } p^{1+\lambda_j}).$$

Combining these two congruences, we have

$$(67) \qquad a_{ij} \equiv (x_i x_j/x_r^2)a_{rr} \qquad (\text{mod } p^{1+\lambda_i}),$$

since $a_{rj}=a_{jr}$. This holds for all $i$, $j=1,\cdots,k$. It follows that $a_{rr}$ is not divisible by $p$; otherwise all $a_{ij}$ would be divisible by $p$. Taking $j=r$ in (67), we find then

$$\nu(a_{ir}) = \lambda_i.$$

In particular, $a_{ir}\neq 0$ for all $i=1,\cdots,k$.

By (64) and $D'D=C$, we have $A^2=p^dA$. Hence

$$\sum_{i=1}^{k} a_{ir}^2 = p^d a_{rr}.$$

Since $a_{ir}\neq 0$, $i=1,\cdots,k$, this yields $(k-1)+a_{rr}^2\leq p^d a_{rr}$. The maximum of $p^d x-x^2$ is obtained for $x=p^d/2$, and thus

$$k - 1 \leq p^{2d}/4$$

which proves our proposition.

## III. Defect groups. Main theorem $A$.

### §1. Blocks of $G$ and those of subgroups

Let $G$ be as before a finite group of order $g=p^a g_0$, $(g_0,p)=1$, where $p$ is a fixed prime number. We consider a pair of subgroups $T$ and $H$ of $G$ satisfying the following two conditions.

(*) For every element $T$ of $T$ there is a $p$-subgroup $P_T$ of $C(T)\cap N(T)$ such that $C(P_T)\subseteq T$,

$$(**) \qquad T \subseteq H \subseteq N(T).$$

For example, the centralizer $T=C(Q)$ of any $p$-subgroup $Q$ of $G$ satisfies (*), if $P_T=Q$ for all $T\in T$. If $H$ is any subgroup of $N(Q)$ containing $T$, the pair $T$, $H$ satisfies (*), (**). Applications of the results below will be made only to pairs $T=C(Q)$, $H$ obtained in this manner.

PROPOSITION 1. *Let $\Omega^*$ be a field of characteristic $p$, and let $T$, $H$ be as above. Then an algebra homomorphism of the class algebra $Z(G,\Omega^*)$ into the class algebra $Z(H,\Omega^*)$ is defined by setting*

$$(1) \qquad \theta : K_\alpha \to K_\alpha^\theta = \sum_{T\in K_\alpha\cap T} T,$$

*where $K_\alpha$ denotes as before the sum of the elements in a conjugate class $K_\alpha$ of $G$.*

PROOF. We denote conjugate classes of $H$ by $L_\rho$. Since $T$ is normal in $H$, the sum in (1) may be expressed as

(2)
$$\sum_{L_\rho \subseteq K_\alpha \cap T} L_\rho$$

where $L_\rho$ is the sum of the elements in $L_\rho$. Thus $K_\alpha^\theta$ is an element of $Z(H,\Omega^*)$, and $\theta$ is at least a linear mapping of $Z(G,\Omega^*)$ into $Z(H,\Omega^*)$. We show that it is an algebra homomorphism. Set

$$K_\alpha^\eta = \sum_{S \in K_\alpha, S \notin T} S$$

so that $K_\alpha = K_\alpha^\theta + K_\alpha^\eta$. If the multiplication of the $K_\alpha$ is given by

(3)
$$K_\alpha K_\beta = \sum_\gamma a_{\alpha\beta\gamma} K_\gamma$$

where each $a_{\alpha\beta\gamma}$ is a non-negative integer, equal to the number of pairs $X \in K_\alpha$, $Y \in K_\beta$ such that $XY$ is a fixed element, say $G_\gamma$ of $K_\gamma$, then we have

(4)
$$(K_\alpha^\theta + K_\alpha^\eta)(K_\beta^\theta + K_\beta^\eta) = \sum_\gamma a_{\alpha\beta\gamma}(K_\gamma^\theta + K_\gamma^\eta).$$

The product $K_\alpha^\theta K_\beta^\theta$ is a sum of elements belonging to $T$ (some with coefficients possibly greater than 1). $K_\alpha^\theta K_\beta^\eta$ is a sum of elements not belonging to $T$, and the same is true of $K_\alpha^\eta K_\beta^\theta$. Furthermore, the coefficient of an element $T$ of $T$ in the product $K_\alpha^\eta K_\beta^\eta$ is a multiple of $p$. Indeed, it is equal to the number of pairs $(X,Y)$ satisfying

$$XY = T;\ X \in K_\alpha,\ X \notin T;\ Y \in K_\beta,\ Y \notin T.$$

If $P$ is an element of the subgroup $P_T$ in (*), then for each pair $(X,Y)$ satisfying the above conditions, the pair $(P^{-1}XP, P^{-1}YP)$ will also satisfy the same conditions. Thus the totality of pairs $(X,Y)$ satisfying the conditions are distributed into classes with respect to transformation by the elements of $P_T$. The number of pairs in such a class is equal to the index $(P_T : P_T \cap C(X) \cap C(Y))$, where $(X,Y)$ is a pair in the class. This index is a power of $p$ distinct from 1, since if it were 1, then we would have $P_T \subseteq C(X)$, whence $X \in C(P_T)$ and $X \in T$ by (*). Being a sum of such indices, the coefficient of $T$ in $K_\alpha^\eta K_\beta^\eta$ is a multiple of $p$ as asserted. Comparing the coefficients of elements of $T$ in both sides of (4), we see that $K_\alpha^\theta K_\beta^\theta$ differs from $\sum_\gamma a_{\alpha\beta\gamma} K^\theta$ by a sum whose coefficients are divisible by $p$. In $Z(H,\Omega^*)$ we then have $K_\alpha^\theta K_\beta^\theta = \sum_\gamma a^*_{\alpha\beta\gamma} K_\gamma^\theta$, where $a^*_{\alpha\beta\gamma}$ is the residue class of $a_{\alpha\beta\gamma}$ (mod $p$), considered as an element of the prime field of $\Omega^*$. Since $K_\alpha K_\beta = \sum_\gamma a^*_{\alpha\beta\gamma} K_\gamma$ in $Z(G,\Omega^*)$ by (3), this shows that our linear mapping $\theta$ is an algebra homomorphism.

The kernel $U$ of the homomorphism $\theta$ has a basis consisting of all $K_\alpha$ such that $K_\alpha \cap T$ is empty. The image $V$ of $\theta$ has a basis consisting of all $K_\alpha^\theta$ such that $K_\alpha \cap T$ is not void. We have the isomorphism

$$(5) \qquad Z(G,\Omega^*)/U \simeq V \qquad (\text{in } Z(H^*,\Omega))$$

induced by $\theta$.

We now let the field $\Omega^*$ be the field $\Omega^* = \mathfrak{o}/\mathfrak{p}$ defined in II, §2. If $\tilde{\psi}$ is a linear character in $\Omega^*$ of the algebra $Z(H,\Omega^*)$, then $\tilde{\psi}$ defines a linear character $\psi$ of $Z(G,\Omega^*)$ by

$$(6) \qquad \psi : Z(G,\Omega^*) \xrightarrow{\theta} V \xrightarrow{\tilde{\psi}} \Omega^*.$$

The kernel of $\psi$ contains the kernel $U$ of $\theta$. If conversely $\psi$ is any linear character of $Z(G,\Omega^*)$ whose kernel contains $U$, then it induces a linear character of $V$ by our isomorphism (5). This linear character of $V$ can be extended to a linear character $\tilde{\psi}$ of $Z(H,\Omega^*)$ by I, §1, Lemma 1. It is evident that this $\tilde{\psi}$ induces our linear character $\psi$ of $Z(G,\Omega^*)$ by (6). Thus we have the first part of

PROPOSITION 2. *For every linear character $\tilde{\psi}$ of $Z(H,\Omega^*)$ we obtain by setting*

$$\psi(K_\alpha) = \tilde{\psi}(K_\alpha^\theta) = \sum_{L_\rho \subseteq K_\alpha \cap T} \tilde{\psi}(L_\rho), \tag{7}$$

*a linear character $\psi$ of $Z(G,\Omega^*)$ whose kernel contains $U$. Conversely, every linear character of $Z(G,\Omega^*)$ whose kernel contains $U$ can be obtained in this manner. By this correspondence $\tilde{\psi}\to\psi$ of linear characters, we obtain a correspondence*

$$\tilde{B} \to B = \tilde{B}^G \tag{8}$$

*from the blocks of $H$ to those of $G$.*

PROOF. Linear characters $\psi$ of $Z(G,\Omega^*)$ are in 1-1 correspondence with blocks of $G$ by II, §8, and similarly, linear characters $\tilde{\psi}$ of $Z(H,\Omega^*)$ are in 1-1 correspondence with blocks of $H$. From our correspondence $\tilde{\psi}\to\psi$ of linear characters, we obtain a correspondence $\tilde{B}\to B$ of blocks. We denote by $\tilde{B}^G$ the image of $\tilde{B}$ under this correspondence.

If $\eta$ denotes Osima's idempotent for the block $B$ of $G$ and if $\eta^*$ denotes its residue class modulo $pZ(G,o)$, the image $\eta^*\theta$ of $\eta^*$ by our homomorphism $\theta$ is an idempotent in $Z(H,\Omega^*)$. Since $\tilde{\psi}(\eta^*\theta) =\psi(\eta^*)$, and this is 1 or 0 according as whether or not the linear character $\psi$ belongs to $B$, this idempotent $\eta^*\theta$, when decomposed into primitive idempotents in $Z(H,\Omega^*)$, is the sum of the residue classes (mod $pZ(H,\mathfrak{o})$) of Osima's idempotents for those blocks $\tilde{B}$ of $H$ satisfying $\tilde{B}^G=B$.

## §2. Defect groups of a block

Let $K_\alpha$ be a conjugate class of $G$. A Sylow $p$-subgroup of the centralizer $C(G_\alpha)$ of any element $G_\alpha$ in $K_\alpha$ will be called a <u>defect group of the class</u> $K_\alpha$. Its order is $p^d$, where $d$ is the defect $\nu(c(G_\alpha))$ of the class $K_\alpha$. Any conjugate in $G$ of a defect group of $K_\alpha$ is also a defect group of $K_\alpha$; conversely, any two defect groups of $K_\alpha$ are conjugate in $G$ by our definition and the Sylow theorems.

Let $B$ be a block of $G$ of defect $d$. If $\psi$ is the linear character of $Z(G,\Omega^*)$ associated with $B$, then there exists by II, Proposition 11, a class $K_\alpha$ of defect $d$ such that $\psi(K_\alpha)\neq 0$. A defect group of such a class $K_\alpha$ is called a <u>defect group of the block</u> $B$.[1] A conjugate of a defect group of $B$ is again a defect group of $B$. As we shall see, the converse is also true. We prove first

PROPOSITION 3. *If $K_\beta$ is a conjugate class satisfying $\psi(K_\beta)$ $\neq 0$ (necessarily of defect $\geq d$ by* II, *Proposition* 11*), then any defect group of the class $K_\beta$ contains a suitable defect group of* $B$.

---

1) Defect groups were first defined in [12]. Their main properties as well as Theorems $A$, $B$ below, were announced in [11], [12], [13]. Detailed proofs are in [20], [22].

PROOF. Let $K_\alpha$ be a class of defect $d$ satisfying $\psi(K_\alpha)\neq 0$. If $K_\alpha K_\beta=\sum_\gamma a_{\alpha\beta\gamma}K_\gamma$ as in (3), then $\psi(K_\alpha)\psi(K_\beta)=\sum_\gamma a^*_{\alpha\beta\gamma}\psi(K_\gamma)$, where $a^*_{\alpha\beta\gamma}$ is the residue class of $a_{\alpha\beta\gamma}$ (mod $p$). Since $\psi(K_\alpha)\neq 0$, $\psi(K_\beta)\neq 0$, so that $\psi(K_\alpha)\psi(K_\beta)\neq 0$, there must exist a class $K_{\gamma_0}$ with

$$(9) \qquad a^*_{\alpha\beta\gamma_0} \neq 0, \qquad \psi(K_{\gamma_0}) \neq 0.$$

By II, Proposition 11, the defect of $K_{\gamma_0}$ is at least equal to $d$. Let $Q$ be a Sylow $p$-subgroup of $C(G_{\gamma_0})$, *i.e.* a defect group of $K_{\gamma_0}$. Set $T=C(Q)$, and let $H$ be any subgroup satisfying $T\subseteq H\subseteq N(Q)$. If $\theta$ is the algebra homomorphism of $Z(G,\Omega^*)$ into $Z(H,\Omega^*)$ considered in the preceding section, then $K_\alpha^\theta K_\beta^\theta=\sum_\gamma a^*_{\alpha\beta\gamma}K_\gamma^\theta$. Since $G_{\gamma_0}\in C(Q)=T$, $K_{\gamma_0}\cap T$ is not empty, hence $K_{\gamma_0}^\theta = \sum_{T\in K_{\gamma_0}\cap T} T\neq 0$. Since $a^*_{\alpha\beta\gamma_0}\neq 0$ by (9), we have

$$K_\alpha^\theta \neq 0, \qquad K_\beta^\theta \neq 0.$$

$K_\alpha^\theta\neq 0$ means that $K_\alpha\cap T$ is not empty, *i.e.* there exists a representative $G_\alpha$ of $K_\alpha$ in $T=C(Q)$, or equivalently, $Q\leq C(G_\alpha)$. Similarly, there exists a representative $G_\beta$ of $K_\beta$ satisfying $Q\leq C(G_\beta)$.

The inclusion $Q\subseteq C(G_\alpha)$ implies $(Q:1)\leq p^{\nu(c(G_\alpha))}=p^d$. But $(Q:1)$ is equal to $p^{\nu(c(G_{\gamma_0}))}$. Hence $\nu(c(G_{\gamma_0}))\leq d$. Together with the opposite inequality established earlier, this gives

$$(10) \qquad \nu(c(G_{\gamma_0})) = d.$$

Therefore the subgroup $Q$ of $C(G_\alpha)$ must be in fact a Sylow $p$-subgroup of $C(G_\alpha)$, and $Q$ is a defect group of the block $B$.

We have thus proved that $C(G_\beta)$ contains a defect group $Q$ of $B$. This shows that some defect group of $K_\beta$ contains a defect group of $B$, and since all defect groups of $K_\beta$ are conjugate, this proves the proposition.

PROPOSITION 4. *Any two defect groups of a block $B$ are conjugate. Conversely, any conjugate of a defect group of $B$ is again one of $B$.*

PROOF. In the above proof of Proposition 3 we proved that if $K_\alpha$ is a class of defect $d$ with $\psi(K_\alpha)\neq 0$, and $K_\beta$ is a class with $\psi(K_\beta)\neq 0$, then there exists an element $G_\alpha$ of $K_\alpha$ and an element $G_\beta$ of $K_\beta$ such that every Sylow $p$-subgroup of $C(G_\beta)$ contains a Sylow $p$-subgroup of $C(G_\alpha)$. If $K_\beta$ is also of defect $d$, then every Sylow $p$-subgroup of $C(G_\beta)$ is actually a Sylow $p$-subgroup of $C(G_\alpha)$. Proposition 4 is now evident.

PROPOSITION 5. *Let $D$ be a defect group of the block $B$ of $G$. Set $T=C(D)$, and let $H$ be any subgroup of $G$ satisfying $T\subseteq H\subseteq N(D)$, i.e. (**) of the preceding section. Then there exists a block $\tilde{B}$ of $H$ such that $B=\tilde{B}^G$ in the sense of Proposition 2 (with respect to the group pair $T,H$).*

PROOF. Let $\psi$ be the linear character of $Z(G,\Omega^*)$ associated with $B$. It suffices to show that the kernel of $\psi$ contains the kernel $U$ of the map $\theta$ of Proposition 1; equivalently, it suffices to show that if $K_\beta$ is a class such that $K_\beta\cap T$ is empty, then $\psi(K_\beta)=0$. Now if $\psi(K_\beta)\neq 0$, then by Proposition 3, 4 we have $D\subseteq C(G_\beta)$, or $G_\beta\in C(D)=T$ for some element $G_\beta$ of $K_\beta$. Therefore there exists a block $\tilde{B}$ of $H$ such that $B=\tilde{B}^G$.

PROPOSITION 6. *Let $T$, $H$ be a pair of subgroups of $G$ satisfying the conditions (*), (**) of the preceding section. If $\tilde{B}$ is a block of $H$, and $B=\tilde{B}^G$ is the block of $G$ corresponding to $\tilde{B}$ in the sense of Proposition 2, then every defect group $\tilde{D}$ of $\tilde{B}$ is contained in a defect group of $B$. In particular, the defect $\tilde{d}$ of $\tilde{B}$ is at most equal to the defect $d$ of $B$.*

PROOF. Let $K_\alpha$ be a class of defect $d$ of $G$ satisfying $\psi(K_\alpha)\neq 0$, where $\psi$ is the linear character of $Z(G,\Omega^*)$ associated with $B$. By the definition of the correspondence $\tilde{B}\to B=\tilde{B}^G$ and formula (7), there exists a class $L_\rho$ in $H$ such that $L_\rho\subseteq K_\alpha\cap T$ and $\tilde{\psi}(L_\rho)\neq 0$, where $\tilde{\psi}$ is the linear character associated with $\tilde{B}$. If $\tilde{G}_\rho\in L_\rho$, then some defect group of $\tilde{B}$ is contained in a Sylow $p$-subgroup of the centralizer $C_H(\tilde{G}_\rho)$ of $\tilde{G}_\rho$ in $H$ by Proposition 3. This Sylow group is contained in a Sylow $p$-subgroup of the centralizer $C(\tilde{G}_\rho)$ in $G$. However, this last Sylow group is a defect group of $B$ since $\tilde{G}_\rho\in K_\alpha$. This and Proposition 4 proves our proposition.

PROPOSITION 7. *Let $M$ be a normal $p$-subgroup of $G$. Then $M$ is contained in every defect group of every block $B$ of $G$.*

PROOF. 1) We consider first a normal subgroup $M$ of $G$ which is not necessarily a $p$-group. Let $\chi^0$ be an irreducible character of the factor group $G^0=G/M$. Using standard notation with the superscript $^0$ for $G^0$, we have

$$\omega^0(G^0) = \frac{g^0}{c^0(G^0)}\,\frac{\chi^0(G^0)}{x^0}$$

Now $\chi^0$ can be considered in a natural way as an irreducible character $\chi$ of $G$ whose kernel contains $M$. If $G^0$ is the coset of $G\in G$, then $C(G)M/M$ is a subgroup of $C^0(G^0)$. Since

$C(G)M/M \simeq C(G)/C(G) \cap M$, we have

(11) $\frac{c(G)}{z(G)} \mid c^0(G^0)$, where $z(G) = (C(G) \cap M:1)$ divides $(M:1)$.

The degree $x^0$ of $\chi^0$ is also the degree $x$ of $\chi$, so that we have

$$\omega^0(G^0) = \frac{g^0}{c^0(G^0)} \frac{\chi(G)}{x} = \frac{g^0}{c^0(G^0)} \cdot \frac{c(G)}{g} \omega(G) = \frac{c(G)}{(M:1)c^0(G^0)} \omega(G), \text{ or}$$

$$(12) \qquad \omega(G) = \frac{(M:1)c^0(G^0)}{c(G)} \omega^0(G^0) = \frac{(M:1)}{z(G)} \frac{c^0(G^0)z(G)}{c(G)} \omega^0(G^0).$$

By (11) both $\frac{(M:1)}{z(G)}$ and $\frac{c^0(G^0)z(G)}{c(G)}$ are integers.

2) Assume now that the normal subgroup $M$ of $G$ is a $p$-group. By II, Proposition 4 $M$ has only one irreducible modular representation, and this must be the 1-representation. Hence any modular representation of $M$ may be taken in the form

$$(13) \qquad \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix}.$$

Consider any irreducible modular representation $F$ of $G$. We may assume that its restriction $F|M$ to $M$ has the form (13). Let $e$ be the first basis element of the representation module $F$ of $F$. Then

$$eM = e \qquad \text{for all } M \in M.$$

For any element $G$ of $G$ we have $GMG^{-1} = M_1 \in M$, and

$$(eG)M = e(GMG^{-1})G = eM_1G = eG.$$

Hence every element $M$ of $M$ leaves fixed all elements of the submodule $F_0$ of $F$ spanned by $\{eG \mid G \in G\}$. Since $F_0$ is a $G$-moudle, and $F$ is irreducible, we have $F_0 = F$, *i.e.*

$$(14) \qquad F|M = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

The kernel of $F$ contains $M$, and $F$ can naturally be considered as an irreducible representation $F^0$ of $G^0=G/M$.

This shows that each block $B$ of $G$ contains at least one irreducible character $\chi$ whose kernel contains $M$ and is thus essentially an irreducible character of $G^0=G/M$. For starting with an irreducible modular representation $F$ in $B$, we may consider it by the above considerations as a representation $F^0$ of $G^0$. We may then take an ordinary irreducible representation $X^0$ of $G^0$ having $F^0$ as a modular constituent, and consider it as an irreducible representation $X$ of $G$.

3) Let $B$ be a block of $G$, and $\chi$ an irreducible character in $B$ whose kernel contains $M$. Consider $\chi$ as an irreducible character $\chi^0$ of $G^0=G/M$. Let $\mathcal{D}$ be a defect group of $B$, and choose an element $G$ of $G$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of $C(G)$ and $\omega(G)\not\equiv 0 \pmod p$. By (12) we then have

$$(15)\qquad \frac{(M:1)}{z(G)} \not\equiv 0,\ \frac{c^0(G^0)z(G)}{c(G)} \not\equiv 0,\ \omega^0(G^0) \not\equiv 0 \qquad \pmod p.$$

In particular, $z(G)=(M:1)$, *i.e.* $(C(G)\cap M:1)=(M:1)$ and $M\subseteq C(G)$. Therefore $M$ is contained in a Sylow $p$-subgroup $\mathcal{D}^{(1)}$ of $C(G)$. Since $D^{(1)}$ is conjugate to $\mathcal{D}$ in $C(G)$, and $M$ is normal in $G$, we have $M\subseteq\mathcal{D}$. This proves the proposition.

Incidentally formula (12) proves that if $B^0$ is a block of a factor group $G^0=G/M$, where $M$ is any normal subgroup of $G$, then all irreducible characters of $G^0$ belonging to $B^0$ belong to a single block of $G$ when they are considered as irreducible characters of $G$. For if $\chi_i^0$, $\chi_j^0$ are two irreducible characters in $B^0$, then $\omega_i^0(G^0)\equiv\omega_j^0(G^0) \pmod p$ for all $G^0\in G^0$. This implies that $\omega_i(G)\equiv \omega_j(G) \pmod p$ for all $G\in G$ by formula (12), or that $\chi_i$ and $\chi_j$

belong to the same block of $G$. Thus every block $B^0$ of $G^0$, when considered as a collection of irreducible characters of $G$, is contained in a single block of $G$. In this sense we have

PROPOSITION 8. *Let $M$ be a normal $p$-subgroup of order $p^\mu$ of $G$. If $B$ is a block of defect $d$ of $G$, and $\mathcal{D}$ is a defect group of $B$, then every block $B^0$ of $G^0=G/M$ which is contained in $B$ has a defect group contained in $\mathcal{D}/M$. Moreover, there exists at least one block $B^0$ of defect $d-\mu$ of $G^0$ contained in $B$ for which $\mathcal{D}/M$ is actually a defect group.*

PROOF. If $G$ is any element of $G$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of $C(G)$, and $\omega(G)\not\equiv 0 \pmod p$, then we have already proved the conditions of (15) hold, where $\chi^0$ is any irreducible character of any block $B^0$ of $G^0$ contained in $B$. The first condition implies that $z(G)=(M:1)=p^\mu$, or $M\subseteq\mathcal{D}$. This together with the second condition $\frac{c^0(G^0)z(G)}{c(G)}\not\equiv 0 \pmod p$ shows that $\mathcal{D}/M$ is a Sylow $p$-subgroup of the centralizer $C^0(G^0)$ of $G^0=GM$ in $G^0$. Since $\omega^0(G^0)\not\equiv 0 \pmod p$ by the third condition of (15), $\mathcal{D}/M$ contains a defect group of $B^0$, which proves the first part of our assertion. In particular, the defect $d^0$ of $B^0$ satisfies $d^0\leq d-\mu$, where $d$ is the defect of $B$.

Now there exists an irreducible modular representation $F$ of $G$ in $B$ whose degree $f$ satisfies

$$\nu(f) = \nu(g) - d = a - d.$$

$F$ can be considered as a representation $F^0$ of $G^0$; if $F^0$ is in the block $B^0$ of $G^0$ of defect $d^0$, then its degree $f^0=f$ satisfies $\nu(f)\geq\nu(g/p^\mu)-d^0=a-\mu-d^0$. Hence $a-d\geq a-\mu-d^0$, *i.e.* $d\leq d^0+\mu$. Hence we have $d^0=d-\mu$. This implies however that $\mathcal{D}/M$ is actually a defect group of the block $B^0$ containing $F^0$. This proves the second part of our assertion.

REMARK. *Consider Proposition 2 in the case of the group pair $T$, $H$, where $T=C(Q)$, $T\subseteq H\subseteq N(Q)$, and $Q$ is a p-subgroup of G (this is the case of later interest). Then the correspondence $\tilde{\psi}\to\psi$ of linear characters is independent of the choice of $Q$ and $T$, and is determined uniquely by the subgroup $H$. Hence the same holds for the correspondence $\tilde{B}\to B=\tilde{B}^G$ of blocks.*

PROOF. The linear character $\psi$ corresponding to $\tilde{\psi}$ is given by (7). To verify our remark we will prove that the sum on the right hand side is

$$\sum_{L_\rho\subseteq K_\alpha\cap H}\tilde{\psi}(L_\rho)$$

where $L_\rho$ runs over all conjugate classes of $H$ contained in $K_\alpha$. This follows simply from the fact that if $L_\rho$ is a conjugate class of $H$ having an empty intersection with $T$, then $\tilde{\psi}(L_\rho)=0$. Namely, if $\tilde{\psi}(L_\rho)\neq 0$, then the centralizer $C_H(\tilde{G}_\rho)$ of any element $\tilde{G}_\rho$ of $L_\rho$ contains a defect group of $\tilde{B}$ by Proposition 3. But every defect group of $\tilde{B}$ contains the normal $p$-subgroup $Q$ of $H$ by Proposition 7. Thus $\tilde{G}_\rho\in C(Q)=T$ and $L_\rho\cap T$ is not empty.

## §3. Main Theorem A

LEMMA 1. *Let $D$ be a p-subgroup of $G$, and let $T=C(\mathcal{D})$, $H=N(\mathcal{D})$.* i) *If $K$ is a conjugate class of $G$ with $\mathcal{D}$ as defect group, then the intersection $K\cap T$ is a conjugate class of $H$.* ii) *If $H$ is an* *element of $H$ such that $\mathcal{D}$ is a Sylow p-subgroup of the centralizer $C_H(H)=C(H)\cap H$ of $H$ in $H$, then $\mathcal{D}$ is a Sylow p-subgroup of $C(H)$; hence* i) *can be applied to the conjugate class $K$ of $H$ in $G$.*

PROOF. i) Let $G$ be an element in $K$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of $C(G)$. Then $G\in T=C(\mathcal{D})$, and $G\in K\cap T$. Let $G'$ be any other element in $K\cap T$. We can put $G'=X^{-1}GX$ with $X\in G$. Since $G'\in T =C(\mathcal{D})$, we have $\mathcal{D}\subseteq C(G')$. Since $\mathcal{D}$ is a Sylow $p$-subgroup of $C(G)$, it follows that $\mathcal{D}$ is a Sylow $p$-subgroup of $C(G')$. On the other hand, $X^{-1}\mathcal{D}X$ is contained in $C(X^{-1}GX)=C(G')$, and so $X^{-1}\mathcal{D}X$ is also a Sylow $p$-subgroup of $C(G')$. Hence $\mathcal{D}$ and $X^{-1}\mathcal{D}X$ are conjugate in $C(G')$, *i.e.* there exists an element $Y$ in $C(G')$ such that $X^{-1}\mathcal{D}X= Y^{-1}\mathcal{D}Y$. We then have $XY^{-1}\in N(\mathcal{D})=H$, and since $(XY^{-1})^{-1}G(XY^{-1})= YG'Y^{-1}=G'$, the element $G'$ is conjugate to $G$ in $H$. Conversely, since $T$ is normal in $H$, any element of $H$ conjugate to $G$ in $H$ belongs to $T$ and hence to $K\cap T$.

ii) Let $\mathcal{D}_1$ be a Sylow $p$-subgroup of $C(H)$ containing $\mathcal{D}$. If $\mathcal{D}_1$ contained $\mathcal{D}$ properly, then by a theorem on $p$-groups, the normalizer of $\mathcal{D}$ in $\mathcal{D}_1$ would provide a $p$-subgroup of $N(\mathcal{D})\cap C(H)=H\cap C(H)$ properly containing $\mathcal{D}$, which would contradict the assumption that $\mathcal{D}$ is a Sylow $p$-subgroup of $C_H(H)$. Hence $\mathcal{D}_1=\mathcal{D}$, and $\mathcal{D}$ is a Sylow $p$-subgroup of $C(H)$.

We now come to

MAIN THEOREM $A$.[1] *Let $\mathcal{D}$ be a p-subgroup of $G$, and let $p^d$ be its order. Then there is a* 1-1 *correspondence between blocks*

---

1) An earlier weaker form of the theorem was announced in [10] as Theorem 4. The proof of its present form appeared in [20].

*of $G$ having $\mathcal{D}$ as defect group and blocks $\tilde{B}$ of defect $d$ of $H=N(\mathcal{D})$. This correspondence is given by the mapping $\tilde{B}\to B=\tilde{B}^G$ of Proposition 2 with respect to the subgroup pair $T=C(\mathcal{D})$, $H=N(\mathcal{D})$.*

PROOF. We remark that by Proposition 7 every block $\tilde{B}$ of defect $d$ of $H=N(\mathcal{D})$ has $\mathcal{D}$ as its unique defect group. The proof of the theorem is in three parts.

1) Let $B$ be a block of $G$ having $\mathcal{D}$ as a defect group. By Proposition 5 there exists a block $\tilde{B}$ of $H$ such that the block $\tilde{B}^G$ of $G$ (in the sense of Proposition 2 with respect to $T$ and $H$) is $B$. By Proposition 6 every defect group of $\tilde{B}$ is contained in a conjugate of $\mathcal{D}$. On the other hand, Proposition 7 shows that every defect group of $\tilde{B}$ contains $\mathcal{D}$. It follows that $\mathcal{D}$ is the in fact unique defect group of $\tilde{B}$, and the defect of $\tilde{B}$ is $d$.

2) Consider any conjugate class $L$ of $H$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of the centralizer $C_H(H)=C(H)\cap H$ in $H$ of some element $H$ in $L$. By our lemma $\mathcal{D}$ is a Sylow $p$-subgroup of $C(H)$ and $L=K\cap C(\mathcal{D})$, where $K$ is the conjugate class of $H$ in $G$. If $\psi$ is the linear character of $Z(G,\Omega^*)$ corresponding to a linear character $\tilde{\psi}$ of $Z(H,\Omega^*)$ in the sense of Proposition 2, we have by (7)

$$\psi(K) = \tilde{\psi}(L) \tag{16}$$

where $K$, $L$ denote as usual the sum of the elements in $K$, $L$ respectively.

In particular let $\tilde{\psi}$ be the linear character associated with a block $\tilde{B}$ of defect $d$ of $H$. As remarked above, $D$ is the unique defect group of $\tilde{B}$. If $L$ is a class of $H$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of $C_H(H)$ for some $H\in L$, and $\tilde{\psi}(L)\neq 0$, then we have (16) for the corresponding linear character $\psi$ and the class $K$ of $H$ in $G$. Since $\tilde{\psi}(L)\neq 0$, it thus follows that $\psi(K)\neq 0$. By Proposition 3 the Sylow $p$-subgroup $\mathcal{D}$ of $C(H)$ contains a defect group of the block $B=\tilde{B}^G$ associated to $\psi$. On the other hand, $D$ is the unique defect group of $\tilde{B}$, and is thus contained in a defect group of $B$ by Proposition 6. It follows that $\mathcal{D}$ is actually a defect group of $B$.

3) Evidently $\tilde{B}$ determines $\tilde{B}^G$ uniquely. In order to prove the converse, namely $\tilde{B}$ is determined uniquely by $\tilde{B}^G$, let $\tilde{B}_1$ be a second block of defect $d$ of $H$ such that $\tilde{B}_1^G=\tilde{B}^G$; $\tilde{B}_1$ has $\mathcal{D}$ as its unique defect group. Let $\tilde{\psi}$, $\tilde{\psi}_1$ be the linear characters of $Z(H,\Omega^*)$ associated with $\tilde{B}$, $\tilde{B}_1$. Consider any conjugate class $L$ of $H$ of defect $d$ in $H$. If $L$ contains no element $H$ such that $\mathcal{D}$ is a Sylow $p$-subgroup of $C_H(H)$, then $\tilde{\psi}(L)=0$, $\tilde{\psi}_1(L)=0$ by Proposition 3. On the other hand, if $L$ contains an element $H$ such that $\mathcal{D}$ is a Sylow subgroup of $C_H(H)$, then by (16) $\tilde{\psi}(L)=\psi(K)$, and similarly, $\tilde{\psi}_1(L)=\psi(K)$. Hence $\tilde{\psi}(L)=\tilde{\psi}_1(L)$ for any class $L$ of defect $d$ in $H$. But then $\tilde{B}_1=\tilde{B}$ by II, Proposition 12 and III, Proposition 3. This shows that $\tilde{B}^G$ unique determines $\tilde{B}$ and the proof is complete.

Theorem $A$ therefore reduces the problem of determining a block with a given defect group to the case where the defect group is a normal subgroup. By Proposition 8, the problem is further reduced to the case of defect 0. For any group it is possible to determine all blocks of defect 0 and their number explicitly (see [20]).

## IV. Generalized Decomposition Numbers. Main Theorem $B$

### §1. Generalized decomposition numbers

Let $G$ be an arbitrary element of $G$, and let $P$, $R$ be its $p$-component and $p$-regular component respectively, so that

$$G = PR = RP.$$

Let $p^{\alpha}$ be the order of $P$. For the subgroup $C(P)$ of $G$ we will use standard notation with a superscript $P$. Thus for instance $X_j^P$ will denote an ordinary irreducible representation of $C(P)$ and $\chi_j^P$ its character. Since $P$ is in the center of $C(P)$, we have $X_j^P(P)=\varepsilon_j I$ for some $p^{\alpha}$-th root $\varepsilon_j$ of 1.

Let $\chi_i$ be an irreducible character of $G$, and let its restriction $\chi_i|C(P)$ to $C(P)$ be $\sum_j a_{ij}\chi_j^P$, where the $a_{ij}$ are non-negative integers. If $\phi_\rho^P$, $d_{j\rho}^P$ denote the irreducible modular characters and decomposition numbers of $C(P)$, we have

$$\chi_i(G) = \chi_i(PR) = \sum_j a_{ij}\chi_j^P(PR)$$
$$= \sum_j a_{ij}\varepsilon_j\chi_j^P(R) = \sum_j a_{ij}\varepsilon_j \sum_\rho d_{j\rho}^P\phi_\rho^P(R).$$

Thus

(1) $$\chi_i(G) = \chi_i(PR) = \sum_\rho \partial_{i\rho}^P\phi_\rho^P(R)$$

where

(2) $$\partial_{i\rho}^P = \sum_j a_{ij}\varepsilon_j d_{j\rho}^P.$$

The numbers $\partial_{i\rho}^P$ are algebraic integers in the field of $p^{\alpha}$-th roots of 1 over the rationals, and are called the generalized decomposition numbers of $G$ with respect to the $p$-element $P$.[1)] Formula (1) holds for any element $G$ with $P$ as its $p$-component. Hence for any $p$-regular element $R$ in $C(P)$, formula (1) holds for $G=PR$. The numbers $\partial^P_{i\rho}$ are uniquely characterized by (1), $R$ ranging over $p$-regular elements of $C(P)$.

The generalized decomposition numbers can be computed explicitly by

$$\partial^P_{i\rho} = \sum_{\kappa,\sigma} \chi_i(PR^P_\kappa) \frac{1}{c(PR^P_\kappa)} \bar{\Phi}^P_\sigma(R^P_\kappa) c^P_{\sigma\rho}, \tag{3}$$

where $R^P_\kappa$ are representatives of the $p$-regular classes $K^P_\kappa$ of $C(P)$, and $c^P_{\sigma\rho}$ are the Cartan invariants of $C(P)$. Indeed, the right hand side of (3) is equal to

$$\begin{aligned}\sum_\kappa \chi_i(PR^P_\kappa) \frac{1}{c(PR^P_\kappa)} \bar{\Phi}^P_\rho(R^P_\kappa) &= \sum_\kappa \sum_\sigma \partial^P_{i\sigma}\phi^P_\sigma(R^P_\kappa) \frac{1}{c(PR^P_\kappa)} \bar{\Phi}^P_\rho(R^P_\kappa) \\ &= \sum_\sigma \partial^P_{i\sigma}\Big(\sum_\kappa \phi^P_\sigma(R^P_\kappa)\frac{1}{c(PR^P_\kappa)}\bar{\Phi}^P_\rho(R^P_\kappa)\Big).\end{aligned}$$

$c(PR^P_\kappa)$ is equal to the order $c^P(R^P_\kappa)$ of the centralizer $C^P(R^P_\kappa)$ of $R^P_\kappa$ in $C(P)$, since $C(PR^P_\kappa)=C(P)\cap C(R^P_\kappa)=C^P(R^P_\kappa)$. Hence the above expression is equal to $\sum_\sigma \partial^P_{i\sigma}\delta_{\rho\sigma}=\partial^P_{i\rho}$, which proves (3).

Letting now $\chi_i$ range over all irreducible characters of $G$, we have the following orthogonality relations.[2)]

$$\sum_i \partial^P_{i\rho}\partial^Q_{i\sigma} = \begin{cases} 0 & \text{if } P,\ Q \text{ are } p\text{-elements not conjugate in } G \\ c^P_{\rho\sigma} & \text{if } P = Q. \end{cases} \tag{4}$$

---

1) Generalized decomposition numbers were introduced in [5], where their elementary properties, including the orthogonality relations (4) below, were proved.

2) Refinements of the relations will be given in §5, Proposition 2.

To prove this, we express (1) as

$$Z^P = \nabla^P \phi^P, \tag{5}$$

where $\nabla^P$ denotes the matrix $(\partial^P_{i\rho})_{i,\rho}$ of generalized decomposition numbers, $Z^P$ denotes the matrix $(\chi_i(PR^P_\kappa))_{i,\kappa}$, and $\phi^P$ denotes the matrix $(\phi^P_\rho(R^P_\kappa))_{\rho,\kappa}$ of modular characters of $C(P)$, $R^P_\kappa$ being representatives of the $p$-regular classes $K^P_\kappa$ in $C(P)$. Similarly we have $Z^Q=\nabla^Q\phi^Q$. Hence

$$(Z^P)'\overline{Z}^Q = (\phi^P)'(\nabla^P)'\overline{\nabla}^Q\overline{\phi}^Q.$$

If $P$ and $Q$ are not conjugate in $G$, then $(Z^P)'Z^Q=0$ by I, (18'), and hence $(\nabla^P)'\overline{\nabla}^Q=0$, since the matrices $\phi^P$, $\phi^Q$ are regular. This proves the first part of (4). If $P=Q$, then

$$(Z^P)'\overline{Z}^P = \begin{pmatrix} \ddots & & 0 \\ & c(PR^P_\kappa) & \\ 0 & & \ddots \end{pmatrix} = \begin{pmatrix} \ddots & & 0 \\ & c^P(R^P_\kappa) & \\ 0 & & \ddots \end{pmatrix} = (\phi^P)'C^P\overline{\phi}^P$$

by I, (18') and II, (15), where $C^P=(c^P_{\sigma\rho})$. Comparing this with the above formula with $P=Q$, we have

$$(\nabla^P)'\overline{\nabla}^P = C^P,$$

which is the second part of (4).

## §2. Sections

Let $P$ be a fixed $p$-element of $G$. The <u>section</u> of $P$ in $G$, denoted by $S(P)$, is defined to be the set of all elements in $G$ having as $p$-component a conjugate in $G$ of $P$. $S(P)$ is thus a collection of conjugate classes of $G$.

LEMMA 1.[1] *Let $P$ be a $p$-element of $G$ in the center of $G$, and $R$ a $p$-regular element of $G$. If $G$ is any element of $G$ not in $S(P)$, then*

$$(6) \qquad \sum_{\chi_i \in B} \chi_i(PR)\overline{\chi}_i(G) = 0$$

*for every block $B$ of $G$.*

PROOF. Let $Q$, $S$ be the $p$-component and the $p$-regular component respectively of $G$. Thus $G=QS$, and since $G \notin S(P)$, the $p$-element $PQ^{-1}$ is different from 1. The left hand side of (6) is equal to

$$\begin{aligned}\sum_{\chi_i \in B} \frac{1}{x}\chi_i(R)\chi_i(P)\chi_i(G^{-1}) &= \sum_{\chi_i \in B} \chi_i(R)\chi_i(PG^{-1}) \\ &= \sum_{\chi_i \in B} \sum_{\phi_\rho \in B} d_{i\rho}\phi_\rho(R)\chi_i(PG^{-1}) \\ &= \sum_{\phi_\rho \in B} \phi_\rho(R)\Phi_\rho(PG^{-1}).\end{aligned}$$

Here $PG^{-1}=PQ^{-1}S^{-1}$ is $p$-singular, since $PQ^{-1} \neq 1$. Hence $\Phi_\rho(PG^{-1})=0$ by II, Proposition 5, and the above sum is 0, which proves (6).

This lemma will be used below in studying certain coefficients connected with Osima's idempotents. Thus for each block $B_\tau$, let $\eta_\tau$ be Osima's idempotent for $B_\tau$. If $K_\alpha$ is the sum of elements in the conjugate class $K_\alpha$ of $G$, and $G_\alpha$ is a representative of $K_\alpha$, we have

$$(7) \qquad \eta_\tau K_\beta = c(G_\beta)^{-1} \sum_{K_\alpha} \sum_{\chi_i \in B_\tau} \chi_i(G_\beta)\overline{\chi}_i(G_\alpha)K_\alpha$$

by I, (24) (this formula has already been used in II, (56)).

---

1) This is a very special case of the Corollary in §5 below.

Set

$$e_{\beta\alpha}^{\tau} = c(G_\beta)^{-1} \sum_{\chi_i \in B_\tau} \chi_i(G_\beta)\overline{\chi}_i(G_\alpha) \tag{8}$$

so that

$$\eta_\tau K_\beta = \sum_{K_\alpha} e_{\beta\alpha}^{\tau} K_\alpha. \tag{9}$$

Under the assumptions of Lemma 1, $e_{\beta\alpha}^{\tau}=e_{\alpha\beta}^{\tau}=0$ whenever $G_\beta$ is $p$-regular element not in $S(P)$ and $G_\alpha$ is in $S(P)$.

If we consider a $p$-element $P$ of $G$ not necessarily lying in the center of $G$, the above lemma can only be applied to the centralizer $C(P)$ of $P$. Thus let $K_\kappa^P$, $\kappa=1,\cdots,k^P$, be the conjugate classes of $C(P)$. We assume that the enumeration is such that the first $\ell^P$, $\kappa=1,\cdots,\ell^P$, are the $p$-regular classes of $C(P)$; as before denote the representatives of these classes by $R_\kappa^P$. The conjugate classes $K_\kappa$ of $G$ containing $PR_\kappa^P$, $\kappa=1,\cdots,\ell^P$, are all distinct, and are exactly the conjugate classes of $G$ lying in the section $S(P)$ of $P$. Let $\tilde{B}_\sigma$ be blocks of $C(P)$, and $\tilde{\eta}_\sigma$ their Osima idempotents. Furthermore, for each block $B_\tau$ of $G$ denote by $\tilde{\eta}^{(\tau)}$ the sum of those $\tilde{\eta}_\sigma$ corresponding to $B_\tau$ in the sense $\tilde{B}_\sigma^G=B_\tau$; if there are no such $\tilde{B}_\sigma$, set $\tilde{\eta}^{(\tau)}=0$. In analogy to (9) we have

$$\tilde{\eta}_\sigma K_\lambda^P = \sum_{\kappa=1}^{k^P} \tilde{e}_{\lambda\kappa}^{\sigma} K_\kappa^P \tag{10}$$

with $\tilde{e}_{\lambda\kappa}^{\sigma}$ defined by formulas analogous to (8). Hence

$$\tilde{\eta}^{(\tau)} K_\lambda^P = \sum_{\kappa=1}^{k^P} \tilde{e}_{\lambda\kappa}^{(\tau)} K_\kappa^P, \tag{11}$$

where $\tilde{e}_{\lambda\kappa}^{(\tau)}$ denotes the sum of those $\tilde{e}_{\lambda\kappa}^{\sigma}$ such that $\tilde{B}_\sigma^G=B_\tau$. The coefficients $\tilde{e}^{\tau}_{\beta\alpha}$, $\tilde{e}^{\sigma}_{\lambda\kappa}$, $\tilde{e}^{(\tau)}_{\lambda\kappa}$ all belong to $\mathfrak{o}$, since Osima's idempotents $\eta_\tau$, $\tilde{\eta}_\sigma$ are $\mathfrak{o}$-linear combinations of $K_\alpha$, $K^P_\kappa$ respectively.

LEMMA 2. *Let* $K_\kappa$, $\kappa=1,\cdots,\ell^P$, *be the conjugate classes of* $G$ *containing* $PK^P_\kappa$, $\kappa=1,\cdots,\ell^P$ *respectively. For* $\lambda$, $\kappa=1,\cdots,\ell^P$ *we have*

$$e^{\tau}_{\lambda\kappa} \equiv e^{(\tau)}_{\lambda\kappa} \quad (\mathrm{mod}\ p). \tag{12}$$

PROOF. (The congruence is in fact an equality, but we shall be able to see this only at the end of the next section.) Consider the image $K^\theta_\lambda$ of $K_\lambda$ under the map $\theta$ defined in III, (1) with $H=T=C(P)$. Clearly

$$K^\theta_\lambda = PK^P_\lambda + \sum_{\substack{K^P_\mu \subseteq K_\lambda \\ K^P_\mu \subsetneq \tilde{S}(P)}} K^P_\mu$$

where $\tilde{S}(P)$ denotes the section of $P$ in $C(P)$. Hence

$$\tilde{\eta}^{(\tau)} K^\theta_\lambda = \tilde{\eta}^{(\tau)} PK^P_\lambda + \sum_{K^P_\mu \subseteq K_\lambda,\, \subsetneq \tilde{S}(P)} \tilde{\eta}^{(\tau)} K^P_\mu .$$

The first product on the right hand side is equal to $\sum\limits_{\kappa=1}^{k^P} \tilde{e}^{(\tau)}_{\lambda\kappa} PK^P_\kappa$ by (11) and in fact to $\sum\limits_{\kappa=1}^{\ell^P} \tilde{e}^{(\tau)}_{\lambda\kappa} PK^P_\kappa$ by the remark made after (9). As for the terms $\tilde{\eta}^{(\tau)} K^P_\mu$ with $K^P_\mu \subsetneq \tilde{S}(P)$, these are linear combinations over $\mathfrak{o}$ of the $K^P_\nu$ satisfying $K^P_\nu \subsetneq \tilde{S}(P)$. This follows from Lemma 1 applied to $C(P)$. Thus we have

$$\tilde{\eta}^{(\tau)} K^\theta_\lambda = \sum_{\kappa=1}^{\ell^P} \tilde{e}^{(\tau)}_{\lambda\kappa} PK^P_\kappa + \sum_{K^P_\nu \subsetneq \tilde{S}(P)} f^{(\tau)}_{\lambda\nu} K^P_\nu \tag{13}$$

for suitable $f^{(\tau)}_{\lambda\kappa} \in \mathfrak{o}$. In $Z(H,\Omega^*)$ consider (13) modulo $pZ(H,\mathfrak{o})$.

Since $\tilde{\eta}^{(\tau)*} = \tilde{\eta}^{(\tau)}$ (mod $pZ(H,o)$) is equal to $\eta_\tau^{*\theta}$ by a remark at the end of III, §1, we obtain

$$(14) \qquad \eta_\tau^{*\theta} K_\lambda^\theta = \sum_{\kappa=1}^{\ell^P} \tilde{e}_{\lambda\kappa}^{(\tau)*} PK_\kappa^P + \sum_{K_\nu^P \lneq \tilde{S}(P)} f_{\lambda\nu}^{(\tau)*} K_\nu^P .$$

The left hand side is equal to $(\eta_\tau^* K_\lambda)^\theta$, since $\theta$ is a homomorphism. By (9) this is in turn equal to

$$\sum_{K_\alpha} e_{\lambda\alpha}^{\tau*} K_\alpha^\theta = \sum_{\alpha=1}^{\ell^P} e_{\lambda\alpha}^{\tau*} PK_\alpha^P + \sum_{\alpha=1}^{k^P} e_{\lambda\alpha}^{\tau*} \sum_{K_\nu^P \subseteq K_\alpha, \lneq \tilde{S}(P)} K_\nu^P .$$

Comparing this with (14), we get $\tilde{e}_{\lambda\kappa}^{(\tau)*} = e_{\lambda\kappa}^{\tau*}$ for $\kappa=1,\cdots,\ell^P$, which is the assertion of Lemma 2.

## §3. The matrix of generalized decomposition numbers

Denote by $B^{(\tau)}$ the collection of all blocks $\tilde{B}_\sigma$ of $C(P)$ satisfying $\tilde{B}_\sigma^G = B_\tau$. If $\nabla_0$ is the submatrix of the matrix $\nabla^P$ in (5) of generalized decomposition numbers defined by

$$(15) \qquad \nabla_0 = (\partial_{i\rho}^P)_{\chi_i \in B_\tau, \phi_\rho^P \in \tilde{B}^{(\tau)}},$$

then we may decompose $\nabla^P$ into

$$(16) \qquad \nabla^P = \begin{pmatrix} \nabla_0 & \nabla_1 \\ \underbrace{\nabla_2}_{B^{(\tau)}} & \nabla_3 \end{pmatrix} \begin{matrix} \} B_\tau \\ \\ \end{matrix}$$

with a suitable enumeration of the $\chi_i$ and $\phi_\rho^P$. The part

$$(\chi_i(PR_\kappa^P))_{\chi_i \in B_\tau, \kappa}$$

of the matrix $Z^P$ in (5) is then equal to

$$(\nabla_0\nabla_1)\phi^P,$$

where $\phi^P$ denotes as in (5) the matrix $(\phi_\lambda^P(R_\kappa^P))_{\lambda,\kappa}$ of modular characters of $C(P)$. By (8) the matrix

(17) $$E_\tau = (e_{\lambda\kappa}^\tau)_{\lambda,\kappa=1,\cdots,\ell^P}$$

of those coefficients $e_{\lambda\kappa}^\tau$ in (9) with indices arising from the section $S(P)$ is equal to

$$\begin{pmatrix} \ddots & & 0 \\ & c(PR_\kappa^P) & \\ 0 & & \ddots \end{pmatrix}^{-1} (\phi^P)' \begin{pmatrix} \nabla_0' \\ \nabla_1' \end{pmatrix} (\overline{\nabla}_0\overline{\nabla}_1)\overline{\phi}^P$$

$$= \begin{pmatrix} \ddots & & 0 \\ & c(PR_\kappa^P) & \\ 0 & & \ddots \end{pmatrix}^{-1} (\phi^P)' \begin{pmatrix} \nabla_0'\overline{\nabla}_0 & \nabla_0'\overline{\nabla}_1 \\ \nabla_1'\overline{\nabla}_0 & \nabla_1'\overline{\nabla}_1 \end{pmatrix} \overline{\phi}^P.$$

Here, as toward the end of §1,

$$\begin{pmatrix} \ddots & & 0 \\ & c(PR_\kappa^P) & \\ 0 & & \ddots \end{pmatrix} = \begin{pmatrix} \ddots & & 0 \\ & c^P(R_\kappa^P) & \\ 0 & & \ddots \end{pmatrix}$$

$$= (\phi^P)'C^P\overline{\phi}^P = (\phi^P)' \begin{pmatrix} C_0^P & 0 \\ 0 & C_1^P \end{pmatrix} \overline{\phi}^P$$

where the matrix $C^P$ of Cartan invariants of $C(P)$ is assumed decomposed into

(18) $$C^P = \begin{array}{c} \begin{pmatrix} C_0^P & 0 \\ \underbrace{0}_{B^{(\tau)}} & C_1^P \end{pmatrix} \end{array} \begin{array}{l} \} \; B_0^{(\tau)} \\ \\ \end{array} .$$

Thus

(19) $$E_\tau = (\overline{\phi}^P)^{-1}\begin{pmatrix} C_0^P & 0 \\ 0 & C_1^P \end{pmatrix}^{-1}(\phi^P)'^{-1}(\phi^P)'\begin{pmatrix} \nabla_0'\overline{\nabla}_0 & \nabla_0'\overline{\nabla}_1 \\ \nabla_1'\overline{\nabla}_0 & \nabla_1'\overline{\nabla}_1 \end{pmatrix}\overline{\phi}^P$$

$$= (\overline{\phi}^P)^{-1}\begin{pmatrix} (C^P)^{-1}\nabla_0'\overline{\nabla}_0 & (C_0^P)^{-1}\nabla_0'\overline{\nabla}_1 \\ (C_1^P)^{-1}\nabla_1'\overline{\nabla}_0 & (C_1^P)^{-1}\nabla_1'\overline{\nabla}_1 \end{pmatrix}\overline{\phi}^P.$$

We next consider the matrix

(20) $$\tilde{E}^{(\tau)} = (\tilde{e}_{\lambda\kappa}^{(\tau)})_{\lambda,\kappa=1,\cdots,\ell^P}.$$

By a similar argument, we have

(21) $$\tilde{E}^{(\tau)} = \begin{pmatrix} \ddots & & 0 \\ & c(PR_\kappa^P) & \\ 0 & & \ddots \end{pmatrix}^{-1}(\phi^P)'\begin{pmatrix} D_0^{P\prime} \\ 0 \end{pmatrix}(D_0^P \quad 0)\overline{\phi}^P$$

$$= \overline{\phi}^{P^{-1}}\begin{pmatrix} C_0^P & 0 \\ 0 & C_1^P \end{pmatrix}^{-1}(\phi^P)'^{-1}(\phi^P)'\begin{pmatrix} C^P & 0 \\ 0 & 0 \end{pmatrix}\overline{\phi}^P$$

$$= (\overline{\phi}^P)^{-1}\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}\overline{\phi}^P,$$

where $D_0^P$ denotes the matrix of decomposition numbers of the characters in $B^{(\tau)}$, and $I$ denotes the identity matrix of the same degree as $C_0^P$.

Since $\overline{\phi}^P$ is obtained from $\phi^P$ by a permutation of the columns, $\overline{\phi}^P$ is a unimodular matrix in $o$. Since $E_\tau$ is a matrix in $o$, it now follows from (19) that $(C_0^P)^{-1}\nabla_0'\overline{\nabla}_0$ is also a matrix in $o$. By Lemma 2 and (21), we now have

(22) $$(C_0^P)^{-1}\nabla_0'\overline{\nabla}_0 \equiv I \qquad (\text{mod } p).$$

This implies in particular that the matrix $(C_0^P)^{-1}\nabla_0'\overline{\nabla}_0$ is unimodular in $o$ and non-singular. Let $\Omega_0$ be the field of $g_0$-th roots of 1 over the rationals $Q$, and let $\Omega_1$ be the field of $p^a$-th roots of 1 over $Q$. Here $g=p^a g_0$ is the order of $G$, and $(g_0,p)=1$. The $\partial^P_{i\rho}$ all belong to $\Omega_1$, while the values of any $\phi^P_j$ belong to $\Omega_0$. If $S$ is any element of the Galois group $\Omega_0\Omega_1/\Omega_0$, then $S$ induces a permutation among the ordinary irreducible characters $\chi_i$, while $S$ leaves invariant the $\phi^P_j$. Thus if $\chi_i \in B_\tau$, then $\chi^S_i$ also belongs to $B_\tau$, since the modular characters of $B_\tau$ are left invariant by $S$. It follows that $S$ induces a permutation among the rows of $\nabla_0$. Each coefficient of the product matrix $\nabla'_0\overline{\nabla}_0$ is then left fixed by $S$ (observe that $S$ commutes with complex conjugation). Thus each coefficient of $\nabla'_0\overline{\nabla}_0$ lies in $\Omega_0$, and hence in $\Omega_0 \cap \Omega_1 = Q$. Thus the *matrix* $\nabla'_0\overline{\nabla}_0$ is rational, and since its coefficients are algebraic integers, they are even rational integers. The matrix $(C^P_0)^{-1}\nabla'_0\overline{\nabla}_0$ is then rational. Since the determinant of the rational, integral matrix $C^P_0$ is a power of $p$ by II, Proposition 13, the coefficients of $(C^P_0)^{-1}\nabla'_0\overline{\nabla}_0$ are rational numbers with powers of $p$ as denominators. On the other hand, we have already seen that they are in $o$. *i.e.* they are $p$-integral. It follows that they are rational integral. We thus have proved

LEMMA 3. *The matrix $(C^P_0)^{-1}\nabla'_0\overline{\nabla}_0$ is rational integral.*

The matrix $\nabla'_0\overline{\nabla}_0$ is positive-definite Hermitian. Indeed for any column $y$ of complex numbers of length equal to the degree of $\nabla'_0\overline{\nabla}_0$, we have $y'\nabla'_0\overline{\nabla}_0\overline{y}\geq 0$; if $y\neq 0$, then $\overline{\nabla}_0\overline{y}\neq 0$ by the non-singularity of $\nabla'_0\overline{\nabla}_0$, and hence $y'\nabla'_0\overline{\nabla}_0\overline{y}>0$. We thus have

$$\det \nabla'_0\overline{\nabla}_0 > 0. \tag{23}$$

Consider now the product $\nabla'_2\overline{\nabla}_2$, where $\nabla_2$ is as in (16). This is also a non-negative hermitian matrix of the same degree. By (4) we have

(24) $$C_0^P = (\nabla_0' \nabla_2') \begin{pmatrix} \overline{\nabla}_0 \\ \overline{\nabla}_2 \end{pmatrix} = \nabla_0' \overline{\nabla}_0 + \nabla_2' \overline{\nabla}_2,$$

so that

(25) $$\det C_0^P \geq \det \nabla_0' \overline{\nabla}_0,$$

the inequality sing holding if $\nabla_2' \overline{\nabla}_2 \neq 0$. Indeed, if $C$ and $U_1$ are positive-definite hermitian matrices of the same degree and $U_2 = C - U_1$ is nonnegative ($U_2$ is necessarily hermitian), then det $C \geq$ det $U_1$, the inequality sign holding if $U_2 \neq 0$. For since $C$ is positive-definite hermitian, there is a non-singular matrix $W$ such that $W' C \overline{W} = I$, or

$$W' U_1 \overline{W} + W' U_2 \overline{W} = I.$$

If $\lambda$ ranges over the eigen-values (*i.e.* characteristic values) of $W' U_1 \overline{W}$, then $1-\lambda$ ranges over those of $I - W' U_1 \overline{W} = W' U_2 \overline{W}$. Hence $1-\lambda \geq 0$ and

$$\det W' U_1 \overline{W} = \Pi \lambda \leq 1.$$

If $U_2 \neq 0$, *i.e.* $W' U_2 \overline{W} \neq 0$, then there exists at least one $\lambda$ with $1-\lambda > 0$ and hence det $W' U_1 \overline{W} < 1$. Multiplication by $((\det W)(\det \overline{W}))^{-1}$ yields our assertion.

We now contend that $\nabla_2' \overline{\nabla}_2$ in fact vanishes. By Lemma 3. det $\nabla_0' \overline{\nabla}_0$ is divisible by det $C_0^P$ and since det $\nabla_0' \overline{\nabla}_0$ is positive, det $\nabla_0' \overline{\nabla}_0 \geq$ det $C_0^P$. However, by (25) we must have det $\nabla_0' \nabla_0 =$ det $C_0^P$, and this implies $\nabla_2' \overline{\nabla}_2 = 0$. This is turn evidently implies

(26) $$\nabla_2 = 0.$$

## §4. Main Theorem $B$

As a consequence of (26) it follows that we must have $\partial_{i\rho}^{P}=0$ for $\chi_i \notin B_\tau$, $\phi_\rho^P \in \tilde{B}^{(\tau)}$. Hence we have proved

MAIN THEOREM $B$. *Let $P$ be a p-element of $G$. Let $B$ be a block of $G$, and $\tilde{B}$ a block of $C(P)$. If $\tilde{B}^G$ is the block of $G$ corresponding to $\tilde{B}$ in the sense of* III, *Proposition* 2 *with respect to the pair $T=H=C(P)$, and $\tilde{B}^G \neq B$, then*

$$\partial_{i\rho}^{P} = 0 \tag{27}$$

*for $\chi_i \in B$ and $\phi_\rho^P \in \tilde{B}$.*

This theorem was announced without proof in [13]. The original proof, somewhat simplified, can be found in [22]. The present proof is based on an idea of Iizuka, [30"].

## §5. Some consequences

We now derive some corollaries of Theorem $B$.

PROPOSITION 1. *Let $\mathcal{D}$ be a defect group of a block $B$ of $G$ and let $\chi_i$ be an irreducible character in $B$. If $P$ is a p-element of $G$, and no conjugate in $G$ of $P$ lies in $\mathcal{D}$, then*

$$\chi_i(PR) = 0 \tag{28}$$

*for any p-regular element $R$ of $C(P)$.*

PROOF. Suppose $\chi_i(PR)\neq 0$. Then $\partial_{i\rho}^{P}\neq 0$ for some irreducible modular character $\phi_\rho^P$ of $C(P)$. If $\tilde{B}$ is the block of $C(P)$ containing $\phi_\rho^P$, then by our main theorem, $\tilde{B}^G=B$. Hence if $\tilde{\mathcal{D}}$ is a defect group of $\tilde{B}$, $\tilde{\mathcal{D}}$ is contained in a conjugate of $\mathcal{D}$ by III, Proposition 6.

On the other hand, the normal subgroup $\{P\}$ of $C(P)$ is contained in $\tilde{D}$ by III, Proposition 7. Thus $\{P\}$ is contained in a conjugate of $\mathcal{D}$, or equivalently, a conjugate of $P$ is contained in $\mathcal{D}$.

In particular, we have

COROLLARY. *If* $\chi$ *is an irreducible character in a block of defect* 0*, then*

$$\chi(G) = 0 \tag{29}$$

*for any p-singular element* $G$.

PROPOSITION 2.[1] *If* $P$*,* $Q$ *are two p-elements of* $G$ *which are not conjugate in* $G$*, then*

$$\sum_{\chi_i \in B} \partial^P_{i\rho} \bar{\partial}^Q_{i\sigma} = 0 \tag{30}$$

*for any block* $B$*, and any irreducible modular characters* $\phi^P_\rho$*,* $\phi^Q_\sigma$ *of* $C(P)$*,* $C(Q)$ *respectively. If* $P=Q$*, then*

$$\sum_{\chi_i \in B} \partial^P_{i\rho} \bar{\partial}^P_{i\sigma} = \begin{cases} c^P_{\rho\sigma} & \text{if } \phi^P_\rho,\ \phi^P_\sigma \text{ belong to the same block } \tilde{B} \text{ of } C(P) \text{ and } \tilde{B}^G = B \\ 0 & \text{otherwise.} \end{cases} \tag{31}$$

PROOF. We know by (4) that

$$\sum_{\tau=1}^{t} \sum_{\chi_i \in B_\tau} \partial^P_{i\rho} \bar{\partial}^Q_{i\sigma} = 0 \tag{32}$$

where $\tau$ runs over the indices for the $t$ blocks of $G$. If $\tilde{B}$ is the block of $C(P)$ containing $\phi^P_\rho$, then $\partial^P_{i\rho}=0$ for all $\chi_i$ not in the block $\tilde{B}^G$ of $G$. Hence (30) is trivially true when $B\neq\tilde{B}^G$. If

1) This refines § 1, (4).

we subtract from (32) these relations for blocks distinct from $\tilde{B}^G$, we obtain (30) for $B=\tilde{B}^G$. The second part of Proposition 2 is similarly proved using Theorem $B$ and (4).

The following corollary generalizes §3, Lemma 1.

COROLLARY. *If $G$, $H$ are elements in two different sections of* $\mathfrak{G}$, *then*

$$\sum_{\chi_i \in B} \chi_i(G)\chi_i(H) = 0 \tag{33}$$

*for any block $B$ of* $\mathfrak{G}$.

PROOF. Let $G=PR$, $H=QS$ be the decomposition of $G$, $H$ into their $p$-components and $p$-regular components. The left hand side of (33) is equal to

$$\sum_{\chi_i \in B} \sum_{\rho} \partial_{i\rho}^{P} \phi_{\rho}^{P}(R) \sum_{\sigma} \overline{\partial}_{i\sigma}^{Q} \overline{\phi}_{\sigma}^{Q}(S) = \sum_{\rho,\sigma} \Big( \sum_{\chi_i \in B} \partial_{i\rho}^{P} \overline{\partial}_{i\sigma}^{Q} \Big) \phi_{\rho}^{P}(R) \overline{\phi}_{\sigma}^{Q}(S)$$

and this is 0 by Proposition 2 if $P$, $Q$ are not conjugate. This corollary is also a consequence of the orthogonality relation I, (18') and the following proposition.

PROPOSITION 3. *Suppose that the relation* $\sum_{\chi_i} a_i \chi_i(G)=0$ *holds for every element $G$ of a section $S(P)$ in* $\mathfrak{G}$, *where the $a_i \in \Omega$ and $\chi_i$ runs over all the irreducible characters of* $\mathfrak{G}$. *Then*

$$\sum_{\chi_i \in B} a_i \chi_i(G) = 0, \qquad G \in S(P) \tag{34}$$

*for any block $B$ of* $\mathfrak{G}$.

PROOF. By our assumption

$$\sum_{\chi_i} \sum_{\rho} \partial_{i\rho}^{P} \phi_{\rho}^{P}(R) a_i = 0$$

for all $p$-regular elements $R$ in $C(P)$. Since the matrix $(\phi_\rho^P(R_\sigma))$, where $\rho$ runs over the indices of the irreducible modular characters of $C(P)$ and $R_\sigma$ over representatives for the $p$-regular classes of $C(P)$, is non-singular, it follows that

$$\sum_{\chi_i} \partial_{i\rho}^P a_i = 0$$

for every $\rho$. As in the proof of Proposition 2, this implies by Theorem $B$ that

$$\sum_{\chi_i \in B} \partial_{i\rho}^P a_i = 0$$

for every block $B$ and for every $\rho$, which in turn implies (50).

COROLLARY. *Let $p$, $q$ be two distinct primes. Let $G$, $H$ be elements of $G$; $P$, $P'$ their $p$-components; and $Q$, $Q'$ their $q$-components. If $P$ does not commute with any conjugate of $Q'$, or if $Q$ does not commute with any conjugate of $P'$, then*

$$\sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G)\overline{\chi}_i(H) = 0$$

*for any $p$-block $B(p)$ and any $q$-block $B'(q)$ of $G$. In particular if $G$ is $p$-singular and $C(P)$ has order prime to $q$, then*

$$\sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G)\overline{\chi}_i(H) = 0$$

*for any $q$-singular element $H$. Furthermore,*

$$\sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G)\chi_i(1) \equiv 0 \pmod{q^b} \tag{35}$$

*where $q^b$ denotes the $q$-component of the order $g$ of $G$.*[1)]

---

1) If $G$ contains no element of order $pq$, then this is the case for every $p$-singular element $G$. Under this assumption (35) was proved in [29].

PROOF. In proving the first part, we may assume that $P$ commutes with no conjugate of $Q'$. It then follows that the $p$-section $S(P)$ of $P$ and the $q$-section $S(Q')$ of $Q'$ have no element in common. By the above Corollary to Proposition 2 (with $q$ in place of $p$) we have

$$\sum_{\chi_i \in B'(q)} \chi_i(G_1)\overline{\chi}_i(H_1) = 0$$

for any element $G_1$ in $S(P)$ and any element $H_1$ in $S(Q')$. For each $H_1 \in S(Q')$ consider this as a character relation $\sum a_i \chi_i$ valid on the $p$-section $S(P)$, where $a_i = \overline{\chi}_i(H_1)$ or 0 according as whether $\chi_i \in B'(q)$ or not. By Proposition 3 we then obtain

$$\sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G_1)\overline{\chi}_i(H_1) = 0$$

for every $G_1 \in S(P)$, which proves the first part of our Corollary.

To prove (35) let $Q$ be a Sylow $q$-subgroup of $G$. If $\psi$ is any character of $Q$, the sum $\sum_{H_1 \in Q} \psi(H_1)$ is a multiple of $q^b$ in the domain of rational integers by I, (10). If $\psi$ is a linear combination of characters of $Q$ with algebraic integers as coefficients, the same is true in the domain of algebraic integers. We apply this to

$$\psi(H_1) = \sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G)\overline{\chi}_i(H_1).$$

where $G$ is fixed and $H_1$ varies in $Q$. We then obtain

$$\sum_{H_1 \in Q} \psi(H_1) = \sum_{H_1 \in Q} \sum_{\chi_i \in B(p) \cap B'(q)} \chi_i(G)\overline{\chi}_i(H_1) \equiv 0 \pmod{q^b}.$$

But by what has already been proved $\psi(H_1)=0$ for $H_1\neq 1$. Hence $\psi(1)=\sum_{\chi_i\in B(p)\cap B'(q)} \chi_i(G)\chi_i(1)\equiv 0 \pmod{q^b}$, which proves (35).

We now return to consideration of blocks for a fixed prime $p$. For any $p$-element $P$ and any block $B_\tau$ of $G$, denote by $\ell_\tau(P)$ the number of irreducible modular characters of $C(P)$ belonging to blocks $\tilde{B}$ of $C(P)$ satisfying $\tilde{B}^G=B_\tau$. As $B_\tau$ ranges over all blocks of $G$, we have

$\sum_{\tau=1}^{t} \ell_\tau(P)$ = number $\ell(P)$ of irreducible modular characters of $C(P)$

= number of $p$-regular conjugate classes of $C(P)$

= number of conjugate classes of $G$ contained in the section $S(P)$.

Thus if $P_1=1,P_2,\cdots,P_r$ form a complete system of representatives of the $p$-classes in $G$, then the sum

$$\sum_{\rho=1}^{r} \ell(P_\rho) = \sum_{\rho=1}^{r} \sum_{\tau=1}^{t} \ell_\tau(P_\rho)$$

is the number $k$ of conjugate classes of $G$. On the other hand, we obviously have

$$k = \sum_{\tau=1}^{t} k_\tau,$$

where $k_\tau$ denotes the number of ordinary irreducible characters in $B_\tau$.

PROPOSITION 4. *For every block $B_\tau$ of $G$*

(36) $$k_\tau = \sum_{\rho=1}^{r} \ell_\tau(P_\rho).$$

PROOF. For each irreducible modular character $\phi_\sigma^{P_\rho}$ of $C(P_\rho)$ define a class function $\phi_\sigma^{(\rho)}$ on $G$ by

$$\phi_\sigma^{(\rho)}(G) = \begin{cases} \phi_\sigma^{P_\rho}(R) & \text{if } G \text{ lies in the section } S(P_\rho)\text{, and } G \\ & \text{is conjugate to } P_\rho R\text{, where } R \text{ is a } p\text{-regu-} \\ & \text{lar element of } C(P_\rho). \\ 0 & \text{otherwise.} \end{cases}$$

If $\chi_i$ is an irreducible character in $B_\tau$, then by (1) and Theorem $B$, $\chi_i$ is a linear combination with coefficients $\partial_{i\sigma}^{P_\rho}$ of those $\phi_\sigma^{(\rho)}$ which belong to blocks $\tilde{B}$ satisfying $\tilde{B}^G = B_\tau$. The total number of these $\phi_\sigma^{(\rho)}$ is the sum $\sum_\rho \ell_\tau(P_\rho)$. Since the number of irreducible characters $\chi_i$ in $B_\tau$ is $k_\tau$, we obtain

$$k_\tau \leq \sum_{\rho=1}^{r} \ell_\tau(P_\rho).$$

But the sum over $\tau=1,\cdots,t$ of each side of the inequality is equal to $k$, as we observed above. Hence the equality sign holds for each $\tau$.

These and many other results indicate that the properties of each $p$-block are closely related to the distribution of $p$-singular elements in $G$. By considering the values of characters for $p$-singular elements as given in (1) by means of the generalized decomposition numbers, Proposition 18 in II, for example, can be further refined; the reader is referred to [23].

For each pair $(\rho,\tau)$ we define the $\ell_\tau(P_\rho)\times\ell(P_\rho)$-matrix $\emptyset_{\rho,\tau}$, the $k_\tau\times\ell_\tau(P_\rho)$-matrix $\nabla_{\rho,\tau}$, and the $k_\tau\times\ell(P_\rho)$-matrix $X_{\rho,\tau}$ as follows:

$\emptyset_{\rho,\tau} = (\phi_\sigma^{P_\rho}(R_\alpha^{P_\rho}))$, where $\phi_\sigma^{P_\rho} \in \tilde{B}$, $\tilde{B}$ ranging over blocks of $C(P_\rho)$ with $\tilde{B}^G = B_\tau$, and $R_\alpha^{P_\rho}$ ranges over representatives of the $p$-regular classes of $C(P_\rho)$,

$\nabla_{\rho,\tau} = (\partial_{i\sigma}^{P_\rho})$, where $\chi_i \in B_\tau$, $\phi_\sigma^{P_\rho} \in \tilde{B}$, $\tilde{B}^G = B_\tau$.

$X_{\rho,\tau} = (\chi_i(P_\rho R_\alpha^{P_\rho}))$, where $\chi_i \in B_\tau$, $R_\alpha^{P_\rho}$ as in $\emptyset_{\rho,\tau}$.

Furthermore, set

$$\emptyset_\tau = \begin{pmatrix} \emptyset_{1,\tau} & & & 0 \\ & \emptyset_{2,\tau} & & \\ & & \ddots & \\ 0 & & & \emptyset_{r,\tau} \end{pmatrix}$$

$$\nabla_\tau = (\nabla_{1,\tau}, \nabla_{2,\tau}, \cdots, \nabla_{r,\tau}),$$

$$X_\tau = (X_{1,\tau}, X_{2,\tau}, \cdots, X_{r,\tau}).$$

In view of Theorem $B$, the relations (1), (5) may be written as

(37) $$X_{\rho,\tau} = \nabla_{\rho,\tau}\emptyset_{\rho,\tau}$$

or

(38) $$X_\tau = \nabla_\tau \emptyset_\tau .$$

Setting

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_t \end{pmatrix}, \quad \nabla = \begin{pmatrix} \nabla_1 & & 0 \\ & \ddots & \\ 0 & & \nabla_t \end{pmatrix}, \quad \emptyset = \begin{pmatrix} \emptyset_1 \\ \vdots \\ \emptyset_t \end{pmatrix},$$

we obtain

(39) $$X = \nabla \emptyset .$$

Hence the matrices $X$, $\nabla$, and $\phi$ are all square matrices of degree $k=\sum_{\tau} k_{\tau}$. Furthermore, with a suitable arrangement of the rows, $\phi$ may be assumed decomposed into submatrices of the irreducible modular characters of $C(P_1)$, $C(P_2),\cdots$, $C(P_r)$. Hence det $\phi \not\equiv 0$ (mod $\mathfrak{p}$). Since $\mathfrak{p}$ can be any prime factor of $p$ in $\Omega$, det $\phi$ is actually prime to $p$. On the other hand, by permuting the rows, $\nabla'\nabla$ can be decomposed into matrices of Cartan invariants by Proposition 2. Hence by II, Proposition 13,

$$(\det \nabla)^2 = \det \nabla'\nabla = \pm \text{ a power of } p.$$

Let $\Omega_0$ be the field of $g_0$-th roots of 1 over the rationals $Q$, and let $\Omega_1$ be the field of $p^{\alpha}$-th roots of 1 over $Q$. As before $(G:1)=g=p^{\alpha}g_0$ with $(p,g_0)=1$. Let $\sigma$ be an element of the Galois group Gal $(\Omega_1/Q)$ of $\Omega_1/Q$. $\sigma$ may also be regarded as an element of Gal $(\Omega_1\Omega_0/\Omega_0)$. Letting $\sigma$ operate on (38), we obtain

$$X_{\tau}^{\sigma} = \nabla_{\tau}^{\sigma}\phi_{\tau}^{\sigma} = \nabla_{\tau}^{\sigma}\phi_{\tau}, \tag{40}$$

since the values of the modular characters lie in $\Omega_0$ by II, §2. It follows that if $\chi_i \in B_{\tau}$, then $\chi_i^{\sigma}$ also belongs to $B_{\tau}$. Hence $\sigma$ induces a permutation among the irreducible characters in $B_{\tau}$. Accordingly, $\nabla_{\tau}^{\sigma}$ is obtained from $\nabla_{\tau}$ by a permutation of its rows, *i.e.*

$$\nabla_{\tau}^{\sigma} = U_{\tau}(\sigma)\nabla_{\tau} \tag{41}$$

for some permutation matrix $U_{\tau}(\sigma)$. On the other hand, there is a rational integer $s$ prime to $p$ such that each $p^{\alpha}$-th root $\varepsilon$ of 1 is sent by $\sigma$ onto its $s$-th power $\varepsilon^{s}$. From (1) we then obtain

$$\chi_i(P^{s}R) = \sum_{\rho}(\partial_{i\rho}^{P})^{\sigma}\phi_{\rho}^{P}(R). \tag{42}$$

If $P^s$ is conjugate to $P_\lambda$, and $P_\lambda = G^{-1}P^sG$ for some $G \epsilon G$, then the map $T \to G^{-1}TG$ as $T$ runs through $C(P)$ gives an isomorphism of $C(P) = C(P^s)$ onto $C(P_\lambda)$. Hence there is a permutation of the indices $\rho = 1, 2, \cdots, \ell_\tau(P) = \ell_\tau(P_\lambda)$ such that

$$\phi_\rho^P(R) = \phi_{\rho'}^{P_\lambda}(G^{-1}RG), \qquad R \ p\text{-regular in } C(P).$$

Putting this into (42) we obtain

$$\chi_i(P^sR) = \sum_\rho (\partial_{i\rho}^P)^\sigma \phi_\rho^P(R) = \sum_\rho (\partial_{i\rho}^P)^\sigma \phi_{\rho'}^{P_\lambda}(G^{-1}RG).$$

But

$$\chi_i(P^sR) = \chi_i(G^{-1}P^sRG) = \chi_i(P_\lambda G^{-1}RG) = \sum_\rho \partial_{i\rho}^{P_\lambda} \phi_\rho^{P_\lambda}(G^{-1}RG).$$

Hence

$$(\partial_{i\rho}^P)^\sigma = \partial_{i\rho'}^{P_\lambda}.$$

This means that $\nabla_\tau^\sigma$ is obtained from $\nabla_\tau$ by a permutation of its columns. If $V_\tau(\sigma)$ is the matrix of this permutation we thus have

$$\nabla_\tau^\sigma = \nabla_\tau V_\tau(\sigma). \tag{43}$$

Together with (41) we have

$$U_\tau(\sigma)\nabla_\tau = \nabla_\tau V_\tau(\sigma). \tag{44}$$

If $\sigma_1$ is a second element of Gal $(\Omega_1/Q)$, then we easily see from (41) and the non-singularity of $\nabla_\tau$ that $U_\tau(\sigma\sigma_1) = U_\tau(\sigma)U_\tau(\sigma_1)$. Similarly, $V_\tau(\sigma_1\sigma) = V_\tau(\sigma\sigma_1) = V_\tau(\sigma_1)V_\tau(\sigma)$. Letting $\sigma$ run over Gal $(\Omega_1/Q)$, we thus get two representations $\sigma \to U_\tau(\sigma)$ and $\sigma \to V_\tau(\sigma)$ of the abelian Galois group Gal $(\Omega_1/Q)$ by permutations; these are equivalent to each other by (44).

Let us call two ordinary irreducible characters $\chi_i$, $\chi_j$ *p-conjugate* if there is an element $\sigma$ of Gal $(\Omega_1\Omega_0/\Omega_0)$ (which is essentially the same as Gal $(\Omega_1/Q)$) such $\chi_i^\sigma=\chi_j$. $p$-conjugate characters are necessarily in the same block.

PROPOSITION 5. *The number of families of p-conjugate irreducible characters in a block $B_\tau$ is equal to the number of families of algebraically conjugate columns of $\nabla_\tau$.*

PROOF. The first number in question is equal to the number of systems of transitivity of the permutation representation $\{U_\tau(\sigma)\}$, and is thus equal to the multiplicity of the 1-representation as a constituent of $\{U_\tau(\sigma)\}$. On the other hand, the generalized decomposition numbers all lie in $\Omega_1$. Thus the second number is equal to the multiplicity of the 1-representation as a constituent in the representation $\{V_\tau(\sigma)\}$. Since the two representations are equivalent, these two numbers are equal.

PROPOSITION 6. *Let $p\neq 2$. There exists a 1-1 correspondence between families of p-conjugate irreducible characters in $B_\tau$ and families of algebraically conjugate columns in $\nabla_\tau$ such that corresponding families consist of the same number of members.*

PROOF. Since $p\neq 2$, Gal $(\Omega_1/Q)$ is cyclic. Let $\sigma$ be a generator. The families of $p$-conjugate irreducible characters in $B_\tau$ are in 1-1 correspondence with the cycles of the permutation $U_\tau(\sigma)$, and indeed, a family consists of $r$ members if and only if the corresponding cycle is of length $r$. Such a cycle of length $r$ corresponds in turn to $r$ distinct $r$-th roots of 1 among the characteristic roots of $U_\tau(\sigma)$. Similarly, each family of algebraically conjugate columns in $\nabla_\tau$ with $r$ members corresponds to $r$ distinct $r$-th roots of 1 among the characteristic roots of $V_\tau(\sigma)$. Since the matrices $U_\tau(\sigma)$ and $V_\tau(\sigma)$ are similar, they have the same characteristic roots. We therefore obtain a 1-1 correspondence as asserted.

PROPOSITION 7. *Let $p \neq 2$. In each $B_\tau$ there exist at least $\ell_\tau$ irreducible characters lying in $\Omega_0$.*

PROOF. Each of the $\ell_\tau$ columns of $\nabla_\tau$ belonging to the section $S(1)$ is rational, and hence constitutes by itself a family of algebraically conjugate columns. By the above proposition, there must exist at least $\ell_\tau$ irreducible characters $\chi_i$ in $B_\tau$, each of which is $p$-conjugate to itself, *i.e.* lies in $\Omega_0$.

REMARK. *For $p=2$ we may obtain analogues of Proposition 6, 7 by replacing the rational field $Q$ by $Q(\sqrt{-1})$. For $p=2$ and $a=1$, 2, Propositions 6, 7 in their original form remain valid.*

## References


[1] K. Asano, Einfacher Beweis einer Brauerschen Satz über Gruppencharaktere, Proc. Jap. Acad., 31 (1955), 501-503.

[2] R. Brauer, Darstellungen der Gruppen in Galoisschen Feldern, Actual. Sci. Ind., 195 (1935).

[3] ________, On modular and $p$-adic representations of algebras, Proc. Nat. Acad. Sci. U.S.A., 25 (1939), 252-258.

[4] ________, On the Cartan invariants of groups of finite order, Ann. Math., 42 (1941), 53-61.

[5] ________, On the connection between the ordinary and modular characters

of groups of finite order, Ann. Math., 42 (1941), 926-935.

[6] ________, Investigations on group characters, Ann. Math., 42 (1941), 936-958.

[7] ________, On groups whose order contains a prime number to the first order I, Amer. J. Math., 64 (1942), 401-420.

[8] ________, On groups whose order contains a prime number to the first order II, Amer. J. Math., 64 (1942), 421-440.

[9] ________, On permutation groups of prime degree and related classes of groups, Ann. Math., 44 (1943), 57-79.

[10] ________, On the arithmetic in a group ring, Proc. Nat. Acad. Sci. U.S.A., 30 (1944), 109-114.

[11] ________, On a conjecture by Nakayama, Trans. Roy. Soc. Canada, 3rd series, 41 (1947), section III, 11-25.

[12] ________, On blocks of characters of groups of finite order, I, Proc. Nat. Acad. Sci. U.S.A., 32 (1946), 182-186.

[13] ________, On blocks of characters of groups of finite order, II, Proc. Nat. Acad. Sci. U.S.A., 32 (1946), 215-219.

[14] ________, On the representation of a finite group of order $g$ in the field of $g$-th roots of unity, Amer. J. Math., 67 (1945), 461-471.

[15] ________, On Artin's $L$-series with general characters, Ann. Math., 48 (1947), 502-514.

[16] ________, Applications of induced characters, Amer. J. Math., 69 (1947), 709-716.

[17] ________, On the algebraic structure of group rings, J. Math. Soc. Japan, 3 (1951), 237-251.

[18] ________, A characterization of the characters of groups of finite order, Ann. Math., 57 (1953), 357-377.

[19] ________, On the structure of groups of finite order, Proc. Internat. Congress Math., (1954), 1-9.

[20] ________, Zur Darstellungstheorie der Gruppen endlicher Ordnung, Math. Zeitschr., 63 (1956), 406-444.

[21] ________, Number theoretical investigations on groups of finite order, Proc. Internat. Symposium, Tokyo-Nikko, (1955), 56-62.

[22] ________, Zur Darstellungstheorie der Gruppen endlicher Ordnung, II, Math. Zeitschr., 72 (1959), 25-46.

[23] R. Brauer-W. Feit, On the number of irreducible characters of finite

groups in a given block, Proc. Nat. Acad. Sci. U.S.A., 45 (1959), 361-365.

[24] R. Brauer-K. A. Fowler, On groups of even order, Ann. Math., 62 (1955), 565-583.

[25] R. Brauer-C. Nesbitt, On the modular representations of groups of finite order, I, Univ. Toronto Studies. Math., Series 4 (1937).

[26] ________________, On the modular characters of groups, Ann. Math., 42 (1941), 556-590.

[27] R. Brauer-W. F. Reynolds, On a problem of E. Artin, Ann. Math., 68 (1958), 713-720.

[27'] R. Brauer-M. Suzuki, On finite groups of even order whose 2-Sylow group is quaternion group, Proc. Nat. Acad. Sci. U.S.A., 45 (1959), 1757-1759.

[28] R. Brauer-M. Suzuki-G. E. Wall, A characterization of the one-dimensional unimodular projective groups over finite fields, Illinois J. Math., 2 (1958), 718-745.

[29] R. Brauer-H. F. Tuan, On simple groups of finite order, I. Bull. Amer. Math. Soc., 51 (1945), 756-766.

[29'] R. Brauer-J. Tate, On the characters of finite groups, Ann. Math., 62 (1955), 1-7.

[30] W. Feit, On a class of doubly transitive permutation groups, Illinois J. Math..

[31] T. Nakayama, Some studies on regular representations, induced representations and modular representations, Ann. Math., 39 (1938), 361-369.

[32] M. Osima, Notes on blocks of group characters, Math. J. Okayama Univ., 4 (1955), 175-188.

[33] P. Roquette, Arithmetische Untersuchung des Charakterrings einer endlichen Gruppe, J. Reine Angew. Math., 190 (1952), 148-168.

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

[33"] R. G. Swan, Induced representations and projective modules, Ann. Math., 71 (1960), 552-578.

[34] M. Suzuki, On finite groups with cyclic Sylow subgroup for all odd primes, Amer. J. Math., 77 (1955), 657-691.

[35] ________, On characterizations of linear groups, I, Trans. Amer. Math. Soc., 92 (1959), 191-204.

[36] ________, On characterizations of linear groups, II, Trans. Amer. Math. Soc., 92 (1959), 205-219.

[37] H. F. Tuan, On groups whose orders contain a prime number to the first power, Ann. Math., 45 (1944), 110-140.

[38] E. Witt, Die algebraische Struktur des Gruppenringes einer endlichen Gruppen über einem Zahlkörper, J. Reine Angew. Math., 190 (1952), 231-245.

Addition of literature

We are planning to add several further papers including

A. Rosenberg, Blocks and centers of groups algebras, Math. Zeitschr., 76 (1961), 209-216.

C. W. Crutis and I. Reiner, Algebras, Groups and Representations, New York 1961.

P. Fong, Some properties of characters of finite solvable groups, Bull. Amer. Math. Soc., 10 (1960).

_______, On the characters of $p$-solvable groups, Trans. Amer. Math. Soc., 98 (1961), 263-284.

## LECTURES IN MATHEMATICS, KYOTO UNIVERSITY

| | | |
|---|---|---|
| No. 1 | Peterson, F. P.—Lectures in Cobordism Theory | $ 5.00 |
| No. 2 | Kubota, T.—On Automorphic Functions and the Reciprocity Law in a Number Field | $ 5.00 |
| No. 3 | Maruyama, M.—On Classification of Ruled Surfaces | $ 5.00 |
| No. 4 | Monsky, P.—p-adic Analysis and Zeta Functions | $ 7.00 |
| No. 5 | Nagata, M.—On Automorphism Group of k[x, y] | $ 5.00 |
| No. 6 | Araki, S.—Typical Formal Groups in Complex Cobordism and K-Theory | $ 5.00 |
| No. 7 | Shin'ya, H.—Spherical Functions and Spherical Matrix Functions on Locally Compacts Groups | $ 5.00 |
| No. 8 | Saito, H.—Automorphic forms and Algebraic Extensions of Number Fields | $ 7.00 |
| No. 9 | Tanaka, N.—A Differential Geometric Study on Strongly Pseudo-Convex Manifolds | $ 7.00 |
| No. 10 | Kambayashi, T. and Miyanishi, M.—On Forms of the Affine Line Over a Field | $ 7.00 |
| No. 11 | Stroock, W. D.—Lectures on Infinite Interacting Systems | $ 7.00 |
| No. 12 | Richard, B.—Theory of Group Characters | $ 7.00 |

Printed by Tokyo Press Co., Ltd., Tokyo, Japan

Printed in Japan