

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.

Copyright © 1979 by Kinokuniya Book-store Co., Ltd.

ALL RIGHT RESERVED

Printed in Japan

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then, these valuable note, based on a series of his lectures at Nagoya University (March-April, 1959), have been kept unpublished.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	page
§1.	Algebras and their representations	1- 8
§2.	Representations of finite groups — classical theory	8-19
§3.	Cyclotomic splitting fields	19-30
II.	Arithmetical Structure	
§1.	The numbers $\omega_i(K_\alpha)$	31
§2.	Modular representations and their characters	32-33
§3.	Transition from an ordinary representation to a modular one	33-34
§4.	Decomposition numbers and Cartan invariants	34-37
§5.	The number of irreducible modular characters	37-39
§6.	The characters ϕ_p	39-41
§7.	The p -rank of the matrix D of decomposition numbers	41-43
§8.	Blocks	43-46
§9.	Idempotents belonging to blocks	46-50
§10.	Defect of a block	50-52
§11.	The determinant of the matrix C of Cartan invariants	52-56
§12.	The elementary divisors of C and C_τ	56-63
§13.	The number of irreducible characters in a block	63-66
III.	Defect groups. Main theorem A	
§1.	Blocks of G and those of subgroups	67-71
§2.	Defect groups of a block	71-78
§3.	Main Theorem A	78-81
IV.	Generalized Decomposition Numbers, Main Theorem B	
§1.	Generalized decomposition numbers	82-84

		page
§2.	Sections	 84-88
§3.	The matrix of generalized decomposition numbers	 88-92
§4.	Main Theorem <i>B</i>	 93
§5.	Some consequences	 93-104
	References	 104-107

I. Preliminaries

§1. Algebras and their representations

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

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

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

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 Ω , 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 Γ give rise to equivalent matrix representations if and only if they are operator-isomorphic with Γ as ring of operators.

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

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

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

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

with irreducible X_i ; the representations $X_1, \dots, X_r$ 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 Γ -subspaces.

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

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

of an algebra Γ is absolutely irreducible, then Γ is said to split. If Γ_Λ splits, Λ is said to be a splitting field of Γ .

An algebra Γ over an algebraically closed field Ω always splits. For if X is an irreducible Γ -module, then the Γ -endomorphism ring of X coincides with Ω , since on the one hand it is a division ring, and on the other hand it is finite-dimensional over Ω as a subring of the full matrix ring of degree $(X:\Omega)$ over Ω . 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 Ω , any algebraically closed extension Λ of Ω will be a splitting field of Γ . From this it follows that Γ always has a splitting field which is of finite degree over Ω . To see this, consider an algebraically closed algebraic extension $\bar{\Omega}$ of Ω , and the finite number of coefficients in those matrices corresponding to a basis of Γ in a complete system of mutually inequivalent irreducible representations of $\Gamma_{\bar{\Omega}}$.

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

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

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 σ in Γ transforming $v_1, \dots, v_m$ to m arbitrarily given elements in X .

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

The subset

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

of Γ is a nilpotent ideal, since $X(N)$ is nilpotent when X is the regular representation (or any faithful representation) of Γ . Conversely, any nilpotent right ideal $\mathfrak{r}$ of Γ 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 $t=1,2,\dots$). Hence N is the largest nilpotent ideal in Γ ; N contains all nilpotent right ideals in Γ and by symmetry, also all nilpotent left ideals in Γ . N is called the radical of Γ .

If the regular representation (or any faithful representation) of Γ is completely reducible, then evidently $N=0$. The converse is true too. Thus, if the radical N of Γ is 0 (Γ is then said to be semi-simple), every simple (*i.e.* irreducible) right ideal $\mathfrak{r}$ of Γ is idempotent and we can then prove that $\mathfrak{r}$ is generated by an idempotent element e in Γ , $\mathfrak{r} = e\Gamma$. 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 Γ is a direct sum

$$(5) \quad \Gamma = \kappa_1 + \dots + \kappa_r$$

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

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

$$(6) \quad \Gamma = \Gamma_1 + \dots + \Gamma_n.$$

This decomposition is even unique up to the order of the summands. If κ is a simple right ideal, then $\Gamma\kappa$ is a sum of right ideals isomorphic to κ ; thus the sum of all right ideals isomorphic to κ and contained in an ideal is again an ideal. Thus all simple right ideals contained in each component Γ_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 Γ_i are in 1-1 correspondence with the distinct irreducible representations of Γ (in Ω). If

$$(7) \quad 1 = \varepsilon_1 + \dots + \varepsilon_n, \quad \varepsilon_i \in \Gamma_i,$$

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

$$(8) \quad Z = Z_1 + \dots + Z_n, \quad Z_i = \varepsilon_i Z.$$

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

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

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

Given a representation X of an algebra Γ , the mapping

$$\chi : \sigma \rightarrow \chi(\sigma) = \text{Tr}X(\sigma)$$

is called the character of Γ 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 Ω is just a homomorphism of the algebra Γ into Ω .

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

LEMMA 1. *Let Γ be a splitting commutative algebra over Ω , and B a subalgebra of Γ . Then any linear character of B in Ω*

may be extended to a character of Γ in Ω .

PROOF. Consider the restriction $X|_B$ to B of the regular representation X of Γ . 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 V of B is contained in $X|_B$. It follows that every irreducible representation of B in Ω is linear and is the restriction of some linear representation of Γ .

§2. Representations of finite groups — classical theory

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

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

of the elements G of G with coefficients a_G in Ω , when we identify a suitable basis of Γ with G itself. Every representation of G in Ω can be uniquely extended to one of Γ , and conversely every representation of Γ in Ω 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 Ω . Its character is given by

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

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

PROPOSITION 1. *If the characteristic $\text{ch}\Omega$ of Ω 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 Ω is completely reducible.*

PROOF. Let λ be the Ω -linear map of Γ to Ω 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 Γ , 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 κ is a non-zero right ideal of Γ , then $\lambda(\kappa) \neq 0$, and $g\lambda(\kappa) \neq 0$. 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 Γ given in (9), and hence $g\lambda(N) = 0$ for the radical N of Γ . This implies by the above remark that $N = 0$. Hence Γ 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 Γ are in Z . Hence, if

$$K_1, K_2, \dots, K_k$$

are the conjugate classes of G , and if for each $i=1, 2, \dots, k$, 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

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

of K_i , $i=1, \dots, k$, over Ω . For this reason Z is thus called the class algebra of G over Ω . If $\text{ch}\Omega$ 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, Ω is algebraically closed, then these fields are all isomorphic to Ω ; their number is necessarily equal to the rank k of $Z(G, \Omega)$ over Ω . By our considerations of the preceding section, we have

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

In particular, if Ω 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 Ω is

a splitting field of G of characteristic 0, then there are exactly k distinct absolutely irreducible representations

$$\chi_1, \chi_2, \dots, \chi_k$$

of G in Ω . Their characters

$$\chi_1, \chi_2, \dots, \chi_k$$

are simply called the irreducible characters of G .

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

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

PROOF. Let χ 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 χ_i (i.e. of χ_i). Now χ is given by (9) as well. Hence for any two elements G, H of G , we have, on setting $\chi_i(G) = (a_{\mu\nu}^{(i)}(G))$,

$$\begin{aligned} \delta_{G,H} &= \frac{1}{g} \chi(GH^{-1}) = \frac{1}{g} \sum_{i=1}^k x_i \chi_i(GH^{-1}) \\ &= \sum_{i=1}^k \sum_{\mu=1}^{x_i} \frac{x_i}{g} a_{\mu\mu}^{(i)}(GH^{-1}) = \sum_{i=1}^k \sum_{\mu, \nu=1}^{x_i} a_{\mu\nu}^{(i)}(G) \frac{x_i}{g} a_{\nu\mu}^{(i)}(H^{-1}). \end{aligned}$$

If we set

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

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 class function 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 Ω forms a k -dimensional vector space over Ω . In A we can introduce an Ω -bilinear inner product

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

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

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

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

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

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

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

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

The orthogonality relation (10) may be expressed also as

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

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

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

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

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

the relation (15) may be written as

$$(16) \quad XN^{-1}\tilde{X}' = I$$

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

$$(17) \quad \tilde{X}'X = N.$$

PROPOSITION 4. *We have*

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

where $\{G_{\kappa}, \kappa=1, \dots, k\}$ 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_{κ} .

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

For each irreducible representation χ_i of G over Ω , the matrix $\chi_i(\zeta)$ is a scalar matrix

$$\chi_i(\zeta) = \omega_i(\zeta)I, \quad \omega_i(\zeta) \in \Omega,$$

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

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

This formula shows that the k linear characters ω_i ($i=1, \dots, k$) of $Z(G, \Omega)$ are linearly independent over Ω , 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 $i=1, \dots, k$, 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 $i=1, \dots, k$, then $\zeta_1 = \zeta_2$.

Next, for each χ_i consider the element

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

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

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

As ω_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

$$(22) \quad \varepsilon_j \varepsilon_\ell = \delta_{j\ell} \varepsilon_j.$$

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

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

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

$$(23) \quad 1 = \sum_{i=1}^k \varepsilon_i.$$

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 ε_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 Ω and $\varepsilon_i \Gamma(G, \Omega)$ is a complete matrix algebra of degree x_i over Ω .

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

$$\begin{aligned}
\omega_i \left(\frac{1}{c(G_\kappa)} \chi_j(G_\kappa) \sum_{\lambda} \chi_j(G_\lambda^{-1}) K_\lambda \right) \\
= \frac{1}{c(G_\kappa)} \chi_j(G_\kappa) \sum_{\lambda} \chi_j(G_\lambda^{-1}) \frac{g}{c(K_\lambda)} \frac{\chi_i(G_\lambda)}{x_i} \\
= \frac{1}{c(G_\kappa)} \chi_j(G_\kappa) \frac{g}{x_i} (\chi_i, \chi_j) = \frac{g}{c(G_\kappa)} \frac{\chi_i(G_\kappa)}{x_i} \delta_{ij}.
\end{aligned}$$

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

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

In the general case of a field Ω 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 Ω is not only a vector space with an inner product defined by (11), but also a commutative Ω -algebra under the usual multiplication $(\theta\psi)(G) = \theta(G)\psi(G)$. Let H be a subgroup of G . The restriction mapping $\theta \rightarrow \theta_H = \theta|_H$ is clearly an Ω -linear homomorphism of $A(G)$ into $A(H)$, the algebra of class functions on H in Ω . 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 $\psi \rightarrow \psi^G$ defined by

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

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

$$(26) \quad \psi^G \theta = (\psi \theta_H)^G,$$

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 θ). We have also the Frobenius reciprocity

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

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

(25)

$$\begin{aligned} (\psi^G, \theta) &= \frac{1}{g} \sum_{G \in G} \psi^G(G) \theta(G^{-1}) = \frac{1}{g} \sum_{G \in G} \frac{1}{h} \sum_{X \in G} \psi_0(XGX^{-1}) \theta(G^{-1}) \\ &= \frac{1}{gh} \sum_{\substack{X \in G \\ H \in H}} \psi(H) \theta(XH^{-1}X) = \frac{1}{h} \sum_{H \in H} \psi(H) \theta(H^{-1}) = (\psi, \theta_H). \end{aligned}$$

It is evident that if θ is a character, then θ_H is one. Furthermore, replacing Ω by a suitable extension if necessary, and letting θ range over the irreducible characters $\chi_1, \dots, \chi_k$ of G , we see that if ψ is a character of H , then ψ^G is one of G ; ψ^G is then called the character of G induced by ψ . In fact, if ψ is the character of a representation Y of H , and if $G_1, \dots, G_r$ form a system of representatives of the right cosets of H in G , then ψ^G is the character of the representation X of G constructed as follows;

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

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

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

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 χ 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

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

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

$$(10') \quad \frac{1}{g} \sum_{G \in G} \chi_i(G) \overline{\chi_j(G)} = \delta_{ij}$$

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

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

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

(24) becomes

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

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

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

in place of (11). This inner product is Hermitian, satisfies $(\theta, \psi) = \overline{(\psi, \theta)}$, and makes the space a Hilbert space. If ψ 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 Ω . For any subring S of Ω 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 $\sum_{\alpha,j} a_{\alpha,j} \psi_{\alpha,j}^G$ with characters $\psi_{\alpha,j}$ of H_α . Secondly U_S is the set of all elements θ in $A(G)$ such that the restriction $\theta|_{H_\alpha}$ belongs to $X_S(H_\alpha)$ for every α . 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 $\psi_{\alpha,j}^G$ is a character of G for every character $\psi_{\alpha,j}$ of H_α , 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),

$$\psi_{\alpha,j}^G \theta = (\psi_{\alpha,j}|_{H_\alpha})^\theta \in X_S(H_\alpha)^G \subseteq V_S$$

for every character $\psi_{\alpha,j}$ of H_α . 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 Ω possesses a $\mathbb{Z}$ -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 $\mathbb{Z}$ -basis be $\{\eta_\mu\}$, say with $\eta_1=1$. The elements η_μ 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 $\chi_1, \dots, \chi_k$, such a relation can be written in the form $\sum_\mu \eta_\mu \sum_i a_{\mu i} \chi_i = 0$ with $a_{\mu i} \in \mathbb{Z}$. But the χ_i are linearly independent over Ω , so that $\sum_\mu \eta_\mu a_{\mu i} = 0$ for $i=1, \dots, k$. Hence $a_{\mu i} = 0$ for all μ, i , and the η_μ are linearly independent over X_Z . Now if $d \in V_S \cap \mathbb{Z}$, then

$$d\eta_1 = d = \sum_{\alpha, j} \psi_{\alpha, j}^G \cdot \sum_\mu z_{\alpha j \mu} \eta_\mu$$

with $\psi_{\alpha, j} \in X_S(H_\alpha)$ and $z_{\alpha j \mu} \in \mathbb{Z}$. 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 ϵ a primitive g -th root of 1. We henceforth set $S = \mathbb{Z}[\epsilon]$. S has a $\mathbb{Z}$ -basis of the form 1, $\epsilon, \dots, \epsilon^{m-1}$ and hence Lemma 2 is applicable with this S .

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

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

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

$$\psi = \sum_v \omega_v(A^{-1}) \omega_v,$$

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 $H \in H$, $H \not\in AB$. We now compute ψ^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_α of the family $\{H_\alpha\}$. Since the induction map is transitive,

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

We now show

PROPOSITION 7. *If the subgroups H_α 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_α 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 ϕ 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 θ satisfies the assumptions of the proposition, then θ is a linear combination with coefficients in S of the various functions ϕ 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_α cover G , then $g \in V_Z$.*

Let p be a fixed prime number. We call an element of G p -regular or p -singular according as to whether or not its order is prime to p . An element whose order is a power of p is called a p -element. 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

$$(32) \quad G = RP = PR$$

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 θ is any element of X_S such that $\theta(G)$ and $\theta(R)$ belong

to Z , then

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

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 χ_i of G are linear, and $\chi_i(G) = \chi_i(P)\chi_i(R)$. If P has order p^μ , this implies that $\chi_i(G)^{p^\mu} = \chi_i(R)^{p^\mu}$. Now θ has the form $\theta = \sum_i a_i \chi_i$, where $a_i \in S$. Raising this equation to the p^μ -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,

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

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

We will call a group H p -elementary 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_α of the family $\{H_\alpha\}$, then there exists an element η 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 η_A of V_S for every $A \in \{A\}$ with the following properties:

$$i) \quad \eta_A(G) \in \mathbb{Z} \text{ for every } G \in G,$$

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

For if such η_A are obtained, we can take η to be the sum $\sum_A \eta_A$. Hence fix $A \in \{A\}$, and let A be the cyclic group generated by A . Let B be a Sylow p -subgroup of the centralizer $C(A)$ of A , and set $H = A \times B$. H is p -elementary and hence is contained in some $H_\alpha \in \{H_\alpha\}$. By Lemma 3 there is an element ϕ of V_S such that $\phi(G) \in \mathbb{Z}$ for every $G \in G$, $\phi(G) = 0$ if G is not conjugate to an element of AB , and $\phi(A) = (C(A):B)$. Since $(C(A):B)$ is prime to p , there is a $z \in \mathbb{Z}$ such that $z(C(A):B) \equiv 1 \pmod{p}$. If we set $\eta_A = z\phi$, then $\eta_A \in V_S$, and η_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 G , then G is not conjugate to an element of AB , and hence ϕ and η_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 G is contained in some group H_α of the family $\{H_\alpha\}$, then $g_0 \in V_Z$, where $g = p^\alpha g_0$ and $(g_0, p) = 1$.*

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

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

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_α of the family $\{H_\alpha\}$, then*

$$(34) \quad U_Z = X_Z(G) = V_Z$$

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

$$(35) \quad U_S = X_S(G) = V_S.$$

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 χ of G can be represented in the form*

$$(36) \quad \chi = \sum a_i \psi_i^*$$

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

a_i is a rational integer.

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

i) θ 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 ψ 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 ψ is primitive, i.e. ψ is not induced by a character of some proper subgroup. Furthermore, by passing to a factor group, we may also assume that ψ is the character of a faithful irreducible representation X over the complex field Ω . 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 Γ_μ all isomorphic to Ω , 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 Γ_μ 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 ψ , 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 Γ_1 and of dimension 1 over Ω . 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 $E \rightarrow E/A$ would be an abelian normal subgroup of E larger than A , since A is central. Thus E is abelian and its irreducible character ψ 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 Ω . X is then contained as an 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 V , 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 χ of X , as well as the characters of every subgroup of G . In particular, if λ is a linear character of a subgroup H of G , and λ^* is the character of G induced by λ , then the representation corresponding to λ^* is realizable in K . Indeed, we may simply take the representation of G induced by the linear representation λ of H . Express now χ in the form (36) of Proposition 9 with the a_i and the ψ_i as described there. If p is any fixed prime, (36) shows that there exists at least one ψ_i^* containing χ with a multiplicity t relatively prime to p . By Lemma 5 ψ_i is induced by a linear character of some subgroup of E_i . Since the process of induction is transitive, the character ψ_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 $\Gamma(G, o)$ of G over a commutative ring o with an identity is defined in the same way as in the case of a group algebra over a field. Its center $Z(G, o)$ consists of all linear combinations over o of the sums K_λ 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 $\Gamma(G_1, \mathbb{Z}), \Gamma(G_2, \mathbb{Z})$ over the rational integers $\mathbb{Z}$ are isomorphic, are then G_1 , and G_2 isomorphic?

II. Arithmetical Structure

§1. The numbers $\omega_i(K_\alpha)$

Let Ω be an algebraic number field, and let Ω_0 be a subring with 1 of Ω . The center $Z(G, \Omega_0)$ of the group ring $\Gamma(G, \Omega_0)$ over Ω_0 is spanned over Ω_0 by the sums $K_1, \dots, K_k$ of the elements of the k conjugate classes of G . Each of the k functions ω_i (I, §2) maps $Z(G, \Omega_0)$ onto a subring of the field generated over Ω_0 by the g -th roots of unity. Indeed the image is a finitely-generated Ω_0 -module, with generators $\omega_i(K_1), \dots, \omega_i(K_k)$. It follows that the image consists of numbers integral over Ω_0 . Taking Ω_0 to be any ring between the ring of rational integers and the ring of algebraic integers in Ω , we have

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

PROPOSITION 2. *For every irreducible character χ_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

$$\sum_{\alpha=1}^k \frac{g}{G(G_\alpha)} \chi_i(G_\alpha) \chi_j(G_\alpha) = g \delta_{ij}, \text{ i.e.}$$

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

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

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

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

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

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

From now on we shall assume that the algebraic number field Ω 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 Ω and Ω^* respectively. If η is in E_0 , and η^* denotes the residue class of $\eta \pmod{\mathfrak{p}}$, then the mapping $\eta \rightarrow \eta^*$ is an isomorphism of E_0 onto the group E_0^* . Indeed, if η, η_1 are two distinct elements of E_0 , the quotient $\frac{\eta}{\eta_1}$ is a g_0 -th root of 1 in Ω

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 $\frac{\eta}{\eta_1} - 1 \nmid g_0$. This is possible only when

$\frac{\eta}{\eta_1} \not\equiv 1 \pmod{p}$, i.e. $\eta \not\equiv \eta_1 \pmod{p}$, 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 Ω^* . Since there are at most g_0 g_0 -th roots of 1

in Ω^* , the mapping $\eta \rightarrow \eta^*$ 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 Ω^* , and let f be its degree. Let R be a p -regular element of G , and let $\epsilon_1^*, \dots, \epsilon_f^*$ be the characteristic roots of $F(R)$. The ϵ_i^* are g_0 -th roots of 1 in Ω^* . By the above remark there exists for each ϵ_i^* one and only one g_0 -th root of 1 in Ω , say ϵ_i , whose residue class (mod p) is ϵ_i^* . We set

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

and call ϕ 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 Ω and not to Ω^* .¹⁾ The residue class $\phi(R)^*$ of $\phi(R)$ (mod p) is the trace $\text{tr } F(R) = \sum_{i=1}^f \epsilon_i^*$ of $F(R)$.

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

Representations over Ω (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 Ω , 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 $e_1, \dots, e_x$ be an Ω -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 $e'_1, \dots, e'_y$, since it is finitely-generated. Indeed, if $e'_1, \dots, e'_y$ are elements of M such that $e'_1, \dots, e'_y \pmod{pM}$ form an $\mathfrak{o}/p = \Omega^*$ basis of the finitely-generated $\mathfrak{o}/p$ -module M/pM , then $e'_1, \dots, e'_y$ generate M over $\mathfrak{o}$ (since p is the Jacobson radical of $\mathfrak{o}$), $e'_1, \dots, e'_y$ are then evidently linearly independent over $\mathfrak{o}$ and over Ω . Since the Ω -module generated by $\{e_\mu G\}$ is X , we have $y=x$, and $e'_1, \dots, e'_x$ form an Ω -basis of X . If we consider the matrix form of X with respect to this new basis $e'_1, \dots, e'_x$, all the matrices $X(G)$, $G \in G$, have coefficients in $\mathfrak{o}$. Passing to their residue classes $\pmod{p}$, we obtain a representation X^* in Ω^* . If we denote the $\mathfrak{o}$ - G -module $\mathfrak{o}e'_1 + \dots + \mathfrak{o}e'_x$ by X_0 , the modular representation X^* corresponds to the representation module X_0/pX_0 over Ω^* .

REMARK. The representation X^* depends on the choice of the Ω -basis $e_1, \dots, e_x$ 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 Ω and Ω^* 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 $F_1, \dots, F_\ell$ be the totality of non-equivalent irreducible modular representations of G (i.e. irreducible representations over Ω^*). Let $\phi_1, \dots, \phi_\ell$ be their characters and $f_1, \dots, f_\ell$ their degrees. Let $X_1, \dots, X_k$ be the totality of non-equivalent irreducible representations of G over Ω (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 $\chi_1, \dots, \chi_k$ and $x_1, \dots, x_k$. Now construct a modular representation X_i^* from each X_i , and denote the multiplicity of F_ρ in X_i^* by $d_{i\rho}$. The non-negative integers $d_{i\rho}$ ($i=1, \dots, k$; $\rho=1, \dots, \ell$) are called the decomposition numbers of G (with respect to p). For a p -regular element R we have

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

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

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

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

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

where

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

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

We call the non-negative integers $c_{\rho\sigma}$ ($\rho, \sigma=1, \dots, \ell$) the Cartan invariants of G (with respect to p).¹⁾ Let

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

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

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

$$(9) \quad C = D'D.$$

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 $\rho=1, \dots, \ell$ an element γ_ρ^* in $\Gamma(G, \Omega^*)$ such that if $F_1, \dots, F_\ell$ are in matrix form, then

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

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

It follows that the traces $\phi_1^*, \dots, \phi_\ell^*$ of $F_1, \dots, F_\ell$ are linearly independent over Ω^* . But each ϕ_ρ^* 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 ϕ_α 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 $\text{tr } F_\rho(G) = \text{tr } F_\rho(R)$, since the characteristic roots of $F_\rho(P)$, being p^ν -th roots of 1 in Ω^* , are all 1. Thus each ϕ_ρ^* is essentially a function of the p -regular classes of G . It follows that the number ℓ is at most equal to the number ℓ_0 of p -regular classes of G , $\ell \leq \ell_0$.

Since $\phi_1^*, \dots, \phi_\ell^*$ are linearly independent over Ω^* , and since they are essentially functions on the p -regular classes, we see that the ℓ modular character $\phi_1, \dots, \phi_\ell$ are linearly independent over $\sigma \pmod{p}$, and hence over σ itself (*i.e.* over Ω). By (5) this yields

PROPOSITION 3. *The decomposition numbers $d_{i\rho}$, the Cartan invariants $c_{\rho\sigma}$, and the characters ϕ_ρ 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 χ_i , there evidently exists at least one ϕ_ρ with $d_{i\rho} \neq 0$. By considering the regular representation, we can also see that for each ϕ_ρ , there exists at least one χ_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

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

and

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

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

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

Now

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

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

$$(14) \quad \phi = (\phi_\rho(G_\alpha)) \quad \rho = 1, \dots, \ell$$

K_α p -regular

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

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

The rank of the matrix on the left hand side is at most equal to ℓ , while the rank of N_r is evidently ℓ_0 by (11). It follows $\ell \geq \ell_0$. Combining this with the inequality obtained in the preceding section, we have

PROPOSITION 4.¹⁾ *The number ℓ of irreducible modular characters of G is equal to the number ℓ_0 of p -regular classes of G ,*

$$\ell = \ell_0.$$

The matrix ϕ 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 $\phi_1, \dots, \phi_\ell$ are linearly independent (mod p),

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

From (15) we have furthermore¹⁾

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

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

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

This can also be expressed as

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

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

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

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

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

§6. The characters ϕ_ρ

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

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

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

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

or

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

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

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

where K_{β} may be p -singular. This we obtain directly from the orthogonality relation I, (18') by (5) and (6). For K_{β} p -singular the right hand side is always 0. Since $\det \phi \neq 0$ we have then $\Phi_{\rho}(G_{\beta}) = 0$ for all ρ . For p -regular K_{β} , 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 $\det \phi \neq 0 \pmod{p}$, this implies $v(\Phi_{\rho}(G_{\beta})) \geq v(c(G_{\beta}))$, $\rho=1, \dots, \ell$.

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

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

Furthermore,

$$(24) \quad v(\Phi_\rho(G)) \geq v(c(G)) \quad \rho = 1, \dots, \ell$$

for any element G of G .

Setting $G=1$, we have in particular $v(\Phi_\rho(1)) \geq v(c(1)) = v(g) = \alpha$.

Thus

PROPOSITION 6. *The degree $\Phi_\rho(1)$ of the character Φ_ρ is divisible by the p -component p^α 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 ℓ ; its rank is exactly ℓ , as we see from (9) and (17). Now we wish to prove

PROPOSITION 7. *The p -rank D is equal to ℓ .*

PROOF. It is sufficient to prove that the p -rank of the matrix $X_p = D\phi$ is equal to ℓ . Suppose that this is less than ℓ . Then there exist ℓ elements μ_α in σ , not all in p , such that

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

for all χ_i . For any σ -linear combination θ of χ_i , we also have

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

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

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

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

ζ_j ranging over the irreducible characters of B . More precisely,

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

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

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

θ 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 Q , and $\theta(G)=0$ when $G \notin H$ (see I, §2). We have

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

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

p -rank of X_p , and hence that of D is equal to ℓ . (Actually we have proved that the p -rank of X_p is not smaller than ℓ_0 . Since $X_p = D\phi$ and ϕ is an $(\ell \times \ell_0)$ -matrix, this implies $\ell \geq \ell_0$. Together with inequality $\ell \leq \ell_0$ 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:

$$(26) \quad 1 = \eta_1^* + \dots + \eta_t^*.$$

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

$$(27) \quad \Gamma^* = \eta_1^* \Gamma^* + \dots + \eta_t^* \Gamma^*,$$

$$(28) \quad Z^* = \eta_1^* Z^* + \dots + \eta_t^* Z^*$$

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

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

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

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

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

To each irreducible character χ_i of G there is associated an algebra homomorphism ω_i of $Z(G, o)$ into o (§1). ω_i induces a linear character ω_i^* : $Z^* = Z(G, o)/pZ(G, o) \rightarrow o/p = \Omega^*$ of Z^* . Hence

$$(30) \quad \omega_i^* = \psi_\tau$$

for some τ , and

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

We distribute the k irreducible characters χ_i into t blocks B_τ by setting

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

That χ_i belongs to the block B_τ is characterized by (31). It is also characterized either by

$$(32) \quad \chi_i^*(\eta_\tau^*) = I$$

or by

$$(33) \quad \chi_i^*(\eta_\sigma^*) = 0 \quad \text{for all } \sigma \neq \tau.$$

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

$$(34) \quad \frac{g}{c(G_\alpha)} \frac{\chi_i(G_\alpha)}{x_i} \equiv \frac{g}{c(G_\alpha)} \frac{\chi_j(G_\alpha)}{x_j} \pmod{p}$$

for all classes K_α in G .

If F_ρ is an irreducible modular constituent of χ_i^* , then by (31),

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

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

$$(36) \quad F_{\rho}(\eta_{\tau}^*) = I$$

or by

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

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

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

$$\phi_{\rho} \in B_{\tau} \implies \phi_{\rho}(G) = \sum_{\chi_i \in B_{\tau}} d_{i\rho} \chi_i(G), \quad G \in G.$$

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

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

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

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

Each ℓ_τ is at least one, *i.e.* every block B_τ contains at least one modular character ϕ_ρ . For if not, the idempotent η_τ^* would be represented in every F_ρ 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_τ contains at least one ordinary irreducible character χ_i . (This can be seen directly by considering the regular representation and (33)). In fact, since the p -rank of D_τ is ℓ_τ ,

$$(39) \quad k_\tau \geq \ell_\tau \geq 1$$

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

§9. Idempotents belonging to blocks

The t idempotents η_τ^* in $Z^* = Z(G, \Omega^*)$ studied in the preceding section are in 1-1 correspondence with the t blocks B_τ . 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 $\epsilon_1, \dots, \epsilon_k$ be the k mutually orthogonal and primitive idempotents in $Z(G, \Omega)$ with the sum $1 = \sum_{i=1}^k \epsilon_i$, these ϵ_i being in 1-1

correspondence with the k irreducible characters $\chi_1, \dots, \chi_k$.
For each block B_τ , set

$$(40) \quad \eta_\tau = \sum_{\chi_i \in B_\tau} \epsilon_i.$$

The t elements $\eta_1, \dots, \eta_t$ 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

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

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

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

PROPOSITION 8. Each η_τ belongs to $Z(G, o)$ and its residue class module $pZ(G, o)$ is the idempotent η_τ^* in (26).

PROOF. For any block B_τ and any class K_α , we have

$$\begin{aligned} (43) \quad b_{\tau\alpha} &= \sum_{\chi_i \in B_\tau} \frac{x_i}{g} \bar{\chi}_i(G_\alpha) = \frac{1}{g} \sum_{\chi_i \in B_\tau} \chi_i(1) \bar{\chi}_i(G_\alpha) \\ &= \frac{1}{g} \sum_{\chi_i \in B_\tau} \left(\sum_{\phi_\rho \in B_\tau} d_{i\rho} \phi_\rho(1) \bar{\chi}_i(G_\alpha) \right) \\ &= \frac{1}{g} \sum_{\phi_\rho \in B_\tau} \left(\sum_{\chi_i \in B_\tau} d_{i\rho} \bar{\chi}_i(G_\alpha) \right) \phi_\rho(1) \\ &= \frac{1}{g} \sum_{\phi_\rho \in B_\tau} \phi_\rho(1) \bar{\phi}_\rho(G_\alpha). \end{aligned}$$

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

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

Here $v(\phi_\rho(1)) \geq v(g) = \alpha$ by Proposition 6, and hence $b_{\tau\alpha} \in o$. This proves $\eta_\tau \in Z(G, o)$.

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

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

In particular $[\eta_\tau]^* \neq 0$ for all τ . Furthermore, since the $[\eta_\tau]^*$ are evidently mutually orthogonal idempotents in $Z(G, o)/pZ(G, o) = Z(G, \Omega^*)$, 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 η_τ^* . Relation (44) implies furthermore that

$$[\eta_\tau]^* = \eta_\tau^*, \quad \tau = 1, \dots, t.$$

Incidentally, we have proved that

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

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

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

where

$$(46) \quad d_\tau = \max_{\phi_\rho \in B_\tau} v\left(\frac{g}{f_\rho}\right).$$

For by (43) we have

$$\begin{aligned}
v(b_{\tau\alpha}) &= v\left(\frac{1}{g} \sum_{\phi_\rho \in B_\tau} \phi_\rho(1)\phi_\rho(G_\alpha)\right) \\
&\geq \text{Min}_{\phi_\rho \in B_\tau} \left(v\left(\frac{f_\rho}{g}\right) + v(\phi_\rho(G_\alpha))\right) \geq \text{Min}_{\phi_\rho \in B_\tau} v(\phi_\rho(G_\alpha)) - d_\tau
\end{aligned}$$

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

§10. Defect of a block

The number d_τ defined in (46) is called the defect of the block B_τ . Thus

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

In other words,

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

As

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

we have clearly $d_\tau \geq \text{Max}_{\chi_i \in B_\tau} v\left(\frac{g}{x_i}\right)$. Actually the equality holds, so

that the defect d_τ may also be defined by means of the degrees of the ordinary irreducible characters χ_i as well as by means of the degrees of the irreducible modular characters ϕ_ρ as in (46). Namely, we have

PROPOSITION 10. *We have*

$$(48) \quad d_{\tau} = \max_{\chi_i \in B_{\tau}} v\left(\frac{g}{x_i}\right).$$

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 ℓ_{τ} of irreducible modular characters ϕ_{ρ} in B_{τ} . The relation (47) then implies $\min_{\chi_i \in B_{\tau}} v(x_i) = \min_{\phi_{\rho} \in B_{\tau}} v(f_{\rho})$, and this proves (48).

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

$$(49) \quad d_G = v(c(G)).$$

The defect of a conjugate class K_{α} of G is defined to be the defect of a representative G_{α} ; 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 χ_i belongs to a block of defect d if and only if $\omega_i(K_{\alpha}) \equiv 0 \pmod{p}$ for all classes K_{α} of defect $< d$, but not for all p -regular classes K_{α} of defect d .*

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

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

There exists an irreducible character χ_j in B_{τ} with $h_j = 0$; for it we have similarly

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

If the class K_α has defect $v(c(G_\alpha)) < d_\tau$, we have $v(\omega_j(K_\alpha)) > 0$, 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

$$1 = \sum_{\substack{K_\alpha \text{ } p\text{-regular} \\ d_{G_\alpha} = d_\tau}} b_{\tau\alpha}^* \omega_i^*(K_\alpha).$$

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

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

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

$$(50) \quad \omega_i^*(\eta_\tau^*) = \sum_{\substack{K_\alpha \text{ } p\text{-regular} \\ \text{class of defect } d}} b_{\tau\alpha}^* \omega_i^*(K_\alpha)$$

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

$$\omega_j^*(\eta_\tau^*) = \sum_{\substack{K_\alpha \text{ } p\text{-regular} \\ \text{class of defect } d}} b_{\tau\alpha}^* \omega_j^*(K_\alpha).$$

So, if $\omega_i(K_\alpha) \equiv \omega_j(K_\alpha) \pmod{p}$ for all p -regular classes K_α of

defect d , then $\omega_i^*(\eta_\tau^*) = \omega_j^*(\eta_\tau^*)$ for every block B_τ of defect d . The last equation holds trivially for every block B_τ of defect $\neq d$, since both sides are 0. Hence $\omega_i^*(\eta_\tau^*) = \omega_j^*(\eta_\tau^*)$ for every block B_τ , and χ_i and χ_j belong to the same block. The converse 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 ϕ 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. θ 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 $P \in \mathcal{P}$, $B \in \mathcal{B}$, we set

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

where ρ is the character of the ordinary regular representation of P . Since the restriction of ϕ to B may be regarded as an ordinary character of B , ψ 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 ϕ_λ , $\lambda=1, \dots, \ell$, be the irreducible modular characters of G (for the prime p). For each $\lambda=1, \dots, \ell$, 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 $a_{i\lambda} \in \mathbb{Z}$, and the χ_i are the ordinary irreducible characters of G . Here

$$\begin{aligned}
a_{i\lambda} &= (\theta_\lambda, \chi_i) = \frac{1}{g} \sum_G \theta_\lambda(G) \overline{\chi}_i(G) = \frac{1}{g} \sum_{G \text{ } p\text{-regular}} \theta_\lambda(G) \overline{\chi}_i(G) \\
&= \frac{1}{g} \sum_{G \text{ } p\text{-regular}} p^a \phi_\lambda(G) \sum_{\mu=1}^{\ell} d_{i\mu} \overline{\phi}_\mu(G) \\
&= p^a \sum_{\mu=1}^{\ell} d_{i\mu} \sum_{G \text{ } p\text{-regular}} \phi_\lambda(G) \frac{1}{g} \overline{\phi}_\mu(G) \\
&= p^a \sum_{\mu=1}^{\ell} d_{i\mu} \sum_{K_\alpha \text{ } p\text{-regular}} \phi_\lambda(G_\alpha) \frac{1}{c(G_\alpha)} \overline{\phi}_\mu(G_\alpha)
\end{aligned}$$

where the $d_{i\mu}$ are the decomposition numbers, and G_α are representatives of the p -regular conjugate classes K_α of G . Since $\phi N_p^{-1} \overline{\phi} = C^{-1}$ 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

$$A = p^a D C^{-1}.$$

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

$$C A' A = p^{2a} C C^{-1} D' D C^{-1} = p^{2a} I,$$

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

The exact value of the determinant of C can now be readily obtained. The determinant of the matrix ϕ in (15) is a unit in the domain $\mathfrak{o}$ of p -integers (*i.e.* the domain of integers for v), and the same is true for the determinant of $\overline{\phi}$, since $\overline{\phi}$ is obtained from ϕ by a permutation of the columns. Hence relation (15) and the form (11) of N_p 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_τ

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 $\mathfrak{o}$, are up to order the p -components of $c(G_1), \dots, c(G_\ell)$. 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 $c(G_1), \dots, c(G_\ell)$. 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 $c(G_1), \dots, c(G_\ell)$.*

Now according to (38), the matrix C breaks up into t parts C_τ corresponding to the t blocks B_τ . The ℓ elementary divisors of C are distributed accordingly into t sets.

PROPOSITION 16. *Assume a fixed enumeration of the ℓ*

irreducible modular characters ϕ_ρ , $\rho=1, \dots, \ell$. For each block B_τ let S_τ be the set of indices ρ with $\phi_\rho \in B_\tau$. We can then enumerate the ℓ p -regular conjugate classes K_σ , such that for each block B_τ , we have

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

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

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

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

Here T runs over all distinct partitions of $1, \dots, \ell$ into t sets T_τ , $\tau=1, \dots, t$, each T_τ consisting of ℓ_τ 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

$$\Delta_1^{(T)} \Delta_2^{(T)} \dots \Delta_t^{(T)} \not\equiv 0 \pmod{p}.$$

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

To prove the second half, fix a block B_τ , and let p^{e_ρ} be the elementary divisors of C_τ , where the indices ρ run through S_τ .

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

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

We may index the rows and columns of U, V by the indices of S_τ .

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 Φ_σ are the characters defined in (6). Then (7) and (52) imply

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

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

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

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)

$$\det(\tilde{\Phi}_\rho(G_\sigma))_{\rho, \sigma \in S_\tau} \not\equiv 0 \pmod{p}.$$

Hence there exists a permutation π_τ of the ℓ_τ indices in S_τ such that $\prod_{\rho \in S_\tau} \tilde{\phi}_\rho(G_{\pi_\tau(\rho)}) \not\equiv 0 \pmod{p}$, or $v(\tilde{\phi}_\rho(G_{\pi_\tau(\rho)})) = 0$ for each $\rho \in S_\tau$.

The inequality (53) gives then

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

We may now suppose that π_τ has been chosen for each τ so that (54) is the case for each τ . But by Proposition 14 the sums of the

left and right hand sides of (54) summed over the block indices $\tau=1, \dots, t$ 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_τ and the elementary divisors of C_τ . Let the multiplication in $Z(G, o)$ of the sums K_α of the elements of the conjugate classes K_α be given by

$$(55) \quad K_\alpha K_\beta = \sum_{\gamma} a_{\alpha\beta\gamma} K_\gamma.$$

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_γ , of K_γ . Clearly we have $a_{\alpha\beta\gamma} = a_{\beta\alpha\gamma}$.

LEMMA 2. *If G_α, G_γ are representatives of K_α, K_γ respectively, and if $v(c(G_\alpha)) < v(c(G_\gamma))$, then $a_{\alpha\beta\gamma} \equiv 0 \pmod{p}$ for any β .*

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_γ . 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_β is the conjugate class consisting of the inverses of the elements of K_β . 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

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

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

$$(57) \quad (\eta_{1,1}^{K_{1,1}}, \dots, \eta_{\tau,\mu}^{K_{\tau,\mu}}, \dots, \eta_{t,\ell_t}^{K_{t,\ell_t}}) \\ = (K_{1,1}, \dots, K_{\tau,\mu}, \dots, K_{t,\ell_t})M,$$

where M is the matrix

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

having the pairs (ω, v) , (τ, μ) as row and column indices respectively. The coefficients of M lie in $\mathcal{o}$, since Osima's idempotents η_τ are $\mathcal{o}$ -linear combinations of the K_α . Furthermore

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

Thus

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

where ϕ is as before the matrix of irreducible modular characters, and ψ is the matrix

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

Since by Proposition 16 $v(\det \overline{\phi})=0$ and $v(\det \psi_\tau)=v(\det C_\tau)+$

$v(\det \phi_\rho(G_{\tau,\mu}))_{\rho \in S_\tau, \mu=1, \dots, \ell_\tau} = v(\prod_{\mu=1}^{\ell_\tau} c(G_{\tau,\mu}))$, we have $v(\det M)=0$,

or $\det M \not\equiv 0 \pmod{p}$. This shows that the $\ell = \sum_{\tau} \ell_\tau$ elements $\eta_{1,1}^{*K_{1,1}}, \dots, \eta_{\tau,\mu}^{*K_{\tau,\mu}}, \dots, \eta_{t,\ell_t}^{*K_{t,\ell_t}}$, 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 Ω^* . In particular, every η_τ^* is a linear combination of the $\eta_{\omega}^* K_{\omega,\nu}$, over Ω^* . But since $\eta_\tau^{*2} = \eta_\tau^*$, in such an expression for η_τ^* , only terms with $\omega=\tau$, i.e. $\eta_\tau^* K_{\tau,\nu}$, $\nu=1, \dots, \ell_\tau$, need be considered. It follows by the above lemma that η_τ^* is a linear combination over Ω^* of those K_α such that $v(c(G_\alpha)) \leq v(c(G_{\tau,\nu}))$ for some class $K_{\tau,\nu}$ associated with B_τ .

We now prove

PROPOSITION 17. *If B_τ is a block of defect $d=d_\tau$, the matrix C_τ has one and only one elementary divisor p^d . All other elementary divisors of C_τ 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_τ a class $K_{\tau,\mu}$ such that $d_\tau \leq v(c(G_{\tau,\mu}))$. Since the p -rank of D_τ is ℓ_τ (§§7,8), there are ℓ_τ ordinary irreducible characters $\chi_{\tau,1}, \dots, \chi_{\tau,\ell_\tau}$ such that the corresponding ℓ_τ rows of D_τ are linearly independent (mod p). Hence by our choice of $K_{\tau,1}, \dots, K_{\tau,\ell_\tau}$

$$(58) \quad \det(\chi_{\tau,i}(G_{\tau,\nu}))_{i,\nu=1,\dots,\ell_\tau} \not\equiv 0 \pmod{p}.$$

Multiply a column, say the ν -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_τ} . On the other hand, the exact power of p dividing the determinant is by

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

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

and this is the case for $v=1, \dots, \ell_{\tau}$. In particular, for the index μ chosen at the beginning of the proof, we thus have

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

This proves our proposition in case $\ell_{\tau}=1$. Assume then $\ell_{\tau} \geq 2$, and consider an index v different from the index μ in (60). Multiply the μ -th and v -th columns of the matrix in (58) by $g/c(G_{\tau,\mu})$ and $g/c(G_{\tau,v})$ respectively. The new μ -th and v -th columns consists of $x_{\tau,i} \omega_{\tau,i}(K_{\tau,\mu})$ and $x_{\tau,i} \omega_{\tau,i}(K_{\tau,v})$ respectively. When divided by $p^{a-d_{\tau}}$, they become the columns $(\frac{x_{\tau,i}}{p} \omega_{\tau,i}(K_{\tau,\mu}))$,

$(\frac{x_{\tau,i}}{p} \omega_{\tau,i}(K_{\tau,v}))$, which are congruent modulo p to

$(\frac{x_{\tau,i}}{p} \omega_{\tau,i}^*(K_{\tau,\mu}))$, $(\frac{x_{\tau,i}}{p} \omega_{\tau,i}^*(K_{\tau,v}))$, 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 $v(g/c(G_{\tau,\mu})) + v(g/c(G_{\tau,v})) = 2a - v(c(G_{\tau,\mu})) - v(c(G_{\tau,v}))$ by (58). Hence

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

and because of (60),

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

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_τ of defect $d=0$. Proposition 17 shows that the corresponding part C_τ of the matrix of Cartan invariants has only one elementary divisor, which is in fact 1. Thus $C_\tau=(1)$. Since D_τ 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_τ be a p -block of defect d . The number k of ordinary irreducible characters χ_i in B_τ satisfies*

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

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

$$(63) \quad a_{ij} = (p^d/g) \sum_{R \text{ } p\text{-regular}} \chi_i(R) \overline{\chi_j(R)}, \quad i, j = 1, \dots, k$$

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.

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

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 $\mathcal{o}$ respectively of degree k, ℓ (ℓ is the number ℓ_τ of irreducible modular character in B) such that

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

where I is the unit matrix of degree ℓ . We have

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

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

$$U_0 A U_0' = p^d \begin{pmatrix} C^{-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

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 χ_i , and ω_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

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

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

$$(66) \quad (g/p^d)(a_{ij}/x_i) \equiv (g/p^d)(a_{rj}/x_r) \pmod{p}.$$

If v is the p -adic exponential valuation with $v(p)=1$, then $v(x_i)=v(g)-d+\lambda_i$, $\lambda_i \geq 0$. Choose χ_r so that $\lambda_r=0$, i.e.

$$v(x_r) = v(g) - d.$$

Then (66) implies the congruence

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

in the ring of p -local integers. Similarly,

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

Combining these two congruences, we have

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

since $a_{rj}=a_{jr}$. This holds for all $i, j=1, \dots, k$. 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

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

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

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

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

Since $a_{ir} \neq 0$, $i=1, \dots, k$, 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 $C(P_T) \subseteq T$,

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

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 Ω^* 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

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

where K_α denotes as before the sum of the elements in a conjugate class K_α of G .

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

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

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

$$K_\alpha^\eta = \sum_{S \in K_\alpha, S \not\subseteq T} S$$

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

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

where each $\alpha_{\alpha\beta\gamma}$ 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_γ of K_γ , then we have

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

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

$$XY = T; X \in K_\alpha, X \not\subseteq T; Y \in K_\beta, Y \not\subseteq T.$$

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 $K_\alpha^n K_\beta^n$ 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 $\sum_Y a_{\alpha\beta Y} K_Y^\theta$ by a sum whose coefficients are divisible by p . In $Z(H, \Omega^*)$ we then have $K_\alpha^\theta K_\beta^\theta = \sum_Y a_{\alpha\beta Y}^* K_Y^\theta$, where $a_{\alpha\beta Y}^*$ is the residue class of $a_{\alpha\beta Y} \pmod{p}$, considered as an element of the prime field of Ω^* . Since $K_\alpha K_\beta = \sum_Y a_{\alpha\beta Y}^* K_Y$ in $Z(G, \Omega^*)$ by (3), this shows that our linear mapping θ is an algebra homomorphism.

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

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

induced by θ .

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

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

The kernel of ψ contains the kernel U of θ . If conversely ψ 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 ψ 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*

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

a linear character ψ 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 $\tilde{\psi} \mapsto \psi$ of linear characters, we obtain a correspondence*

$$(8) \quad \tilde{B} \mapsto B = \tilde{B}^G$$

from the blocks of H to those of G .

PROOF. Linear characters ψ 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 $\tilde{\psi} \mapsto \psi$ of linear characters, we obtain a correspondence $\tilde{B} \mapsto B$ of blocks. We denote by $\tilde{B}^G$ the image of $\tilde{B}$ under this correspondence.

If η denotes Osima's idempotent for the block B of G and if η^* denotes its residue class modulo $pZ(G, o)$, the image $\eta^*\theta$ of η^* by our homomorphism θ 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 ψ 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_α be a conjugate class of G . A Sylow p -subgroup of the centralizer $C(G_\alpha)$ of any element G_α in K_α will be called a defect group of the class K_α . Its order is p^d , where d is the defect $v(e(G_\alpha))$ of the class K_α . Any conjugate in G of a defect group of K_α is also a defect group of K_α ; conversely, any two defect groups of K_α are conjugate in G by our definition and the Sylow theorems.

Let B be a block of G of defect d . If ψ is the linear character of $Z(G, \Omega^*)$ associated with B , then there exists by II, Proposition 11, a class K_α of defect d such that $\psi(K_\alpha) \neq 0$. A defect group of such a class K_α is called a defect group of the block 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_β 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_β 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_α be a class of defect d satisfying $\psi(K_\alpha) \neq 0$. If $K_\alpha K_\beta = \sum_Y a_{\alpha\beta Y} K_Y$ as in (3), then $\psi(K_\alpha)\psi(K_\beta) = \sum_Y a_{\alpha\beta Y}^* \psi(K_Y)$, where $a_{\alpha\beta Y}^*$ is the residue class of $a_{\alpha\beta Y} \pmod{p}$. 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_{Y_0} with

$$(9) \quad a_{\alpha\beta Y_0}^* \neq 0, \quad \psi(K_{Y_0}) \neq 0.$$

By II, Proposition 11, the defect of K_{Y_0} is at least equal to d .

Let Q be a Sylow p -subgroup of $C(G_{Y_0})$, i.e. a defect group of K_{Y_0} . Set $T = C(Q)$, and let H be any subgroup satisfying $T \subseteq H \subseteq N(Q)$.

If θ is the algebra homomorphism of $Z(G, \Omega^*)$ into $Z(H, \Omega^*)$ considered in the preceding section, then $K_\alpha^\theta K_\beta^\theta = \sum_Y a_{\alpha\beta Y}^* K_Y^\theta$. Since $G_{Y_0} \in C(Q) = T$, $K_{Y_0} \cap T$ is not empty, hence $K_{Y_0}^\theta = \sum_{T \in K_{Y_0} \cap T} T \neq 0$. Since $a_{\alpha\beta Y_0}^* \neq 0$ by (9), we have

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

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

The inclusion $Q \leq C(G_\alpha)$ implies $(Q:1) \leq p^{v(c(G_\alpha))} = p^d$. But $(Q:1)$ is equal to $p^{v(c(G_{Y_0}))}$. Hence $v(c(G_{Y_0})) \leq d$. Together with the opposite inequality established earlier, this gives

$$(10) \quad v(c(G_{Y_0})) = d.$$

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_β contains a defect group of B , and since all defect groups of K_β 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_α is a class of defect d with $\psi(K_\alpha) \neq 0$, and K_β is a class with $\psi(K_\beta) \neq 0$, then there exists an element G_α of K_α and an element G_β of K_β such that every Sylow p -subgroup of $C(G_\beta)$ contains a Sylow p -subgroup of $C(G_\alpha)$. If K_β 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 $\mathcal{D}$ be a defect group of the block B of G . Set $T=C(\mathcal{D})$, and let H be any subgroup of G satisfying $T \subseteq H \subseteq N(\mathcal{D})$, 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 ψ be the linear character of $Z(G, \Omega^*)$ associated with B . It suffices to show that the kernel of ψ contains the kernel U of the map θ of Proposition 1; equivalently, it suffices to show that if K_β 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 $\mathcal{D} \subseteq C(G_\beta)$, or $G_\beta \in C(\mathcal{D})=T$ for some element G_β of K_β . 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_α be a class of defect d of G satisfying $\psi(K_\alpha) \neq 0$, where ψ is the linear character of $Z(G, \Omega^*)$ associated with B . By the definition of the correspondence $\tilde{B} \rightarrow B = \tilde{B}^G$ and formula (7), there exists a class L_ρ 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 χ^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 χ^0 can be considered in a natural way as an irreducible character χ 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

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

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

The degree x^0 of χ^0 is also the degree x of χ , so that we have

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

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

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

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

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

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

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 -module, and F is irreducible, we have $F_0 = F$, i.e.

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

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 χ 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 χ an irreducible character in B whose kernel contains M . Consider χ as an irreducible character χ^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

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

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 $\mathcal{D}^{(1)}$ 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 χ_i^0, χ_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 χ_i and χ_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^μ 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 χ^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 $\frac{e^0(G^0)z(G)}{e(G)} \not\equiv 0 \pmod{p}$ 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

$$v(f) = v(g) - d = a - d.$$

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 $v(f) \geq v(g/p^\mu) - d^0 = a - \mu - d^0$. 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 $\tilde{\psi} \rightarrow \psi$ 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 $\tilde{B} \rightarrow B = \tilde{B}^G$ of blocks.

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

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

where L_p runs over all conjugate classes of H contained in K_α . This follows simply from the fact that if L_p is a conjugate class of H having an empty intersection with T , then $\tilde{\psi}(L_p) = 0$. Namely, if $\tilde{\psi}(L_p) \neq 0$, then the centralizer $C_H(\tilde{G}_p)$ of any element $\tilde{G}_p$ of L_p 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 $\tilde{G}_p \in C(Q) = T$ and $L_p \cap T$ is not empty.

§3. Main Theorem A

LEMMA 1. Let $\mathcal{D}$ 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 $\tilde{B} \rightarrow B = \tilde{B}^G$ 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 ψ 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)

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

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, $\mathcal{D}$ 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 ψ 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 ψ . On the other hand, $\mathcal{D}$ 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 $\tilde{B}^G$ uniquely 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^α be the order of P . For the subgroup $C(P)$ of G we will use standard notation with a superscript P . Thus for instance χ_j^P will denote an ordinary irreducible representation of $C(P)$ and χ_j^P its character. Since P is in the center of $C(P)$, we have $\chi_j^P(P) = \epsilon_j I$ for some p^α -th root ϵ_j of 1.

Let χ_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

$$\begin{aligned} \chi_i(G) &= \chi_i(PR) = \sum_j a_{ij} \chi_j^P(PR) \\ &= \sum_j a_{ij} \epsilon_j \chi_j^P(R) = \sum_j a_{ij} \epsilon_j \sum_\rho d_{j\rho}^P \phi_\rho^P(R). \end{aligned}$$

Thus

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

where

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

The numbers $\partial_{i\rho}^P$ are algebraic integers in the field of p^α -th roots of 1 over the rationals, and are called the generalized decomposition

sition 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 $\partial_{i\rho}^P$ are uniquely characterized by (1), R ranging over p -regular elements of $C(P)$.

The generalized decomposition numbers can be computed explicitly by

$$(3) \quad \partial_{i\rho}^P = \sum_{\kappa, \sigma} \chi_i(PR_\kappa^P) \frac{1}{c(PR_\kappa^P)} \frac{1}{\phi_\sigma^P(R_\kappa^P)} c_{\sigma\rho}^P,$$

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

$$\begin{aligned} \sum_{\kappa} \chi_i(PR_\kappa^P) \frac{1}{c(PR_\kappa^P)} \frac{1}{\phi_\rho^P(R_\kappa^P)} &= \sum_{\kappa} \sum_{\sigma} \partial_{i\sigma}^P \phi_\sigma^P(R_\kappa^P) \frac{1}{c(PR_\kappa^P)} \frac{1}{\phi_\rho^P(R_\kappa^P)} \\ &= \sum_{\sigma} \partial_{i\sigma}^P \left(\sum_{\kappa} \phi_\sigma^P(R_\kappa^P) \frac{1}{c(PR_\kappa^P)} \phi_\rho^P(R_\kappa^P) \right). \end{aligned}$$

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

Letting now χ_i range over all irreducible characters of G , we have the following orthogonality relations.²⁾

$$(4) \quad \sum_i \partial_{i\rho}^P \partial_{i\sigma}^Q = \begin{cases} 0 & \text{if } P, Q \text{ are } p\text{-elements not} \\ & \text{conjugate in } G \\ c_{\rho\sigma}^P & \text{if } P = Q. \end{cases}$$

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

$$(5) \quad Z^P = \nabla^P \phi^P,$$

where ∇^P denotes the matrix $(\partial_{i\rho}^P)_{i,\rho}$ of generalized decomposition numbers, Z^P denotes the matrix $(\chi_i(PR_\kappa^P))_{i,\kappa}$, and ϕ^P denotes the matrix $(\phi_\rho^P(R_\kappa^P))_{\rho,\kappa}$ of modular characters of $C(P)$, R_κ^P being representatives of the p -regular classes K_κ^P in $C(P)$. Similarly we have $Z^Q = \nabla^Q \phi^Q$. Hence

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

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

$$(Z^P)' \bar{Z}^P = \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & c(PR_\kappa^P) & & \\ 0 & & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & c^P(R_\kappa^P) & & \\ 0 & & \cdot & \cdot \end{pmatrix} = (\phi^P)' c^P \bar{\phi}^P$$

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

$$(\nabla^P)' \bar{\nabla}^P = c^P,$$

which is the second part of (4).

§2. Sections

Let P be a fixed p -element of G . The section 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

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

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 $G \not\in S(P)$, 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_τ , let η_τ be Osima's idempotent for B_τ . If K_α is the sum of elements in the conjugate class K_α of G , and G_α is a representative of K_α , we have

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

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

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

so that

$$(9) \quad \eta_{\tau} K_{\beta} = \sum_{K_{\alpha}} e_{\beta\alpha}^{\tau} K_{\alpha}.$$

Under the assumptions of Lemma 1, $e_{\beta\alpha}^{\tau} = e_{\alpha\beta}^{\tau} = 0$ whenever G_{β} is p -regular element not in $S(P)$ and G_{α} 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_{κ}^P , $\kappa=1, \dots, k^P$, be the conjugate classes of $C(P)$. We assume that the enumeration is such that the first l^P , $\kappa=1, \dots, l^P$, are the p -regular classes of $C(P)$; as before denote the representatives of these classes by R_{κ}^P . The conjugate classes K_{κ} of G containing PR_{κ}^P , $\kappa=1, \dots, l^P$, 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_{τ} of G denote by $\tilde{\eta}^{(\tau)}$ the sum of those $\tilde{\eta}_{\sigma}$ corresponding to B_{τ} 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

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

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

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

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 $\tilde{e}_{\beta\alpha}^\tau$, $\tilde{e}_{\lambda\kappa}^\sigma$, $\tilde{e}_{\lambda\kappa}^{(\tau)}$ all belong to σ , since Osima's idempotents η_τ , $\tilde{\eta}_\sigma$ are σ -linear combinations of K_α , K_κ^P respectively.

LEMMA 2. Let K_κ , $\kappa=1, \dots, l^P$, be the conjugate classes of G containing PK_κ^P , $\kappa=1, \dots, l^P$ respectively. For λ , $\kappa=1, \dots, l^P$ we have

$$(12) \quad e_{\lambda\kappa}^\tau \equiv e_{\lambda\kappa}^{(\tau)} \pmod{p}.$$

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_λ^θ of K_λ under the map θ defined in III, (1) with $H=T=C(P)$. Clearly

$$K_\lambda^\theta = PK_\lambda^P + \sum_{\substack{K_\mu^P \subseteq K_\lambda \\ K_\mu^P \notin \tilde{S}(P)}} K_\mu^P$$

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

$$\tilde{\eta}^{(\tau)} K_\lambda^\theta = \tilde{\eta}^{(\tau)} PK_\lambda^P + \sum_{K_\mu^P \subseteq K_\lambda, K_\mu^P \notin \tilde{S}(P)} \tilde{\eta}^{(\tau)} K_\mu^P.$$

The first product on the right hand side is equal to $\sum_{\kappa=1}^{l^P} \tilde{e}_{\lambda\kappa}^{(\tau)} PK_\kappa^P$

by (11) and in fact to $\sum_{\kappa=1}^{l^P} \tilde{e}_{\lambda\kappa}^{(\tau)} PK_\kappa^P$ by the remark made after (9).

As for the terms $\tilde{\eta}^{(\tau)} K_\mu^P$ with $K_\mu^P \notin \tilde{S}(P)$, these are linear combinations over σ of the K_ν^P satisfying $K_\nu^P \notin \tilde{S}(P)$. This follows from Lemma 1 applied to $C(P)$. Thus we have

$$(13) \quad \tilde{\eta}^{(\tau)} K_\lambda^\theta = \sum_{\kappa=1}^{l^P} \tilde{e}_{\lambda\kappa}^{(\tau)} PK_\kappa^P + \sum_{K_\nu^P \notin \tilde{S}(P)} f_{\lambda\nu}^{(\tau)} K_\nu^P$$

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

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

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

The left hand side is equal to $(\eta_\tau^{*} K_\lambda)^\theta$, since θ is a homomorphism.

By (9) this is in turn equal to

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

Comparing this with (14), we get $\tilde{e}_{\lambda\kappa}^{(\tau)*} = e_{\lambda\kappa}^{\tau*}$ for $\kappa=1, \dots, \ell^P$, 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 ∇_0 is the submatrix of the matrix ∇^P in (5) of generalized decomposition numbers defined by

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

then we may decompose ∇^P into

$$(16) \quad \nabla^P = \left(\begin{array}{cc} \nabla_0 & \nabla_1 \\ \nabla_2 & \nabla_3 \end{array} \right) \}_{B_\tau}^{B^{(\tau)}}$$

with a suitable enumeration of the χ_i and ϕ_ρ^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 ϕ^P denotes as in (5) the matrix $(\phi_\lambda^P(R_\kappa^P))_{\lambda, \kappa}$ of modular characters of $\mathcal{C}(P)$. By (8) the matrix

$$(17) \quad E_\tau = (e_{\lambda\kappa}^\tau)_{\lambda, \kappa=1, \dots, l^P}$$

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

$$\begin{aligned} & \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & \cdot & \cdot & \\ & \cdot & \cdot & \\ 0 & & & \cdot \end{pmatrix}^{-1} (\phi^P), \begin{pmatrix} \nabla_0' \\ \nabla_1' \end{pmatrix} (\overline{\nabla}_0 \overline{\nabla}_1) \overline{\phi}^P \\ &= \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & \cdot & \cdot & \\ & \cdot & \cdot & \\ 0 & & & \cdot \end{pmatrix}^{-1} (\phi^P), \begin{pmatrix} \nabla_0' \overline{\nabla}_0 & \nabla_0' \overline{\nabla}_1 \\ \nabla_1' \overline{\nabla}_0 & \nabla_1' \overline{\nabla}_1 \end{pmatrix} \overline{\phi}^P. \end{aligned}$$

Here, as toward the end of §1,

$$\begin{aligned} & \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & \cdot & \cdot & \\ & \cdot & \cdot & \\ 0 & & & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & 0 \\ & \cdot & \cdot & \\ & \cdot & \cdot & \\ 0 & & & \cdot \end{pmatrix} \\ &= (\phi^P), C_{\phi}^{P-P} = (\phi^P), \begin{pmatrix} C_0^P & 0 \\ 0 & C_1^P \end{pmatrix} \overline{\phi}^P \end{aligned}$$

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

$$(18) \quad C^P = \begin{pmatrix} C_0^P & 0 \\ 0 & C_1^P \end{pmatrix} \Big\}_{B_0^{(\tau)}}^{B^{(\tau)}}.$$

Thus

$$\begin{aligned}
(19) \quad E_\tau &= (\bar{\phi}^P)^{-1} \begin{pmatrix} c_0^P & 0 \\ 0 & c_1^P \end{pmatrix}^{-1} (\phi^P)^{-1} (\phi^P)^{-1} \begin{pmatrix} \nabla_0' \bar{\nabla}_0 & \nabla_0' \bar{\nabla}_1 \\ \nabla_1' \bar{\nabla}_0 & \nabla_1' \bar{\nabla}_1 \end{pmatrix} \bar{\phi}^P \\
&= (\bar{\phi}^P)^{-1} \begin{pmatrix} (c_0^P)^{-1} \nabla_0' \bar{\nabla}_0 & (c_0^P)^{-1} \nabla_0' \bar{\nabla}_1 \\ (c_1^P)^{-1} \nabla_1' \bar{\nabla}_0 & (c_1^P)^{-1} \nabla_1' \bar{\nabla}_1 \end{pmatrix} \bar{\phi}^P.
\end{aligned}$$

We next consider the matrix

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

By a similar argument, we have

$$\begin{aligned}
(21) \quad \tilde{E}^{(\tau)} &= \begin{pmatrix} \cdot & \cdot & 0 \\ & \cdot & \\ & c(PR_\kappa^P) & \\ 0 & & \cdot \end{pmatrix}^{-1} (\phi^P)^{-1} \begin{pmatrix} D_0^P & \\ & 0 \end{pmatrix} (D_0^P \quad 0) \bar{\phi}^P \\
&= \bar{\phi}^P^{-1} \begin{pmatrix} c_0^P & 0 \\ 0 & c_1^P \end{pmatrix}^{-1} (\phi^P)^{-1} (\phi^P)^{-1} \begin{pmatrix} c^P & 0 \\ 0 & 0 \end{pmatrix} \bar{\phi}^P \\
&= (\bar{\phi}^P)^{-1} \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \bar{\phi}^P,
\end{aligned}$$

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 $\bar{\phi}^P$ is obtained from ϕ^P by a permutation of the columns, $\bar{\phi}^P$ is a unimodular matrix in σ . Since E_τ is a matrix in σ , it now follows from (19) that $(c_0^P)^{-1} \nabla_0' \bar{\nabla}_0$ is also a matrix in σ . By Lemma 2 and (21), we now have

$$(22) \quad (c_0^P)^{-1} \nabla_0' \bar{\nabla}_0 \equiv I \pmod{p}.$$

This implies in particular that the matrix $(c_0^P)^{-1} \nabla_0' \bar{\nabla}_0$ is unimodular in σ and non-singular. Let Ω_0 be the field of g_0 -th roots

of 1 over the rationals Q , and let Ω_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 $\phi_{i\rho}^P$ all belong to Ω_1 , while the values of any ϕ_j^P belong to Ω_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 χ_i , while S leaves invariant the ϕ_j^P . Thus if $\chi_i \in B_\tau$, then χ_i^S also belongs to B_τ , since the modular characters of B_τ are left invariant by S . It follows that S induces a permutation among the rows of ∇_0 . Each coefficient of the product matrix $\nabla_0' \bar{\nabla}_0$ is then left fixed by S (observe that S commutes with complex conjugation). Thus each coefficient of $\nabla_0' \bar{\nabla}_0$ lies in Ω_0 , and hence in $\Omega_0 \cap \Omega_1 = Q$. Thus the matrix $\nabla_0' \bar{\nabla}_0$ is rational, and since its coefficients are algebraic integers, they are even rational integers. The matrix $(c_0^P)^{-1} \nabla_0' \bar{\nabla}_0$ is then rational. Since the determinant of the rational, integral matrix c_0^P is a power of p by II, Proposition 13, the coefficients of $(c_0^P)^{-1} \nabla_0' \bar{\nabla}_0$ are rational numbers with powers of p as denominators. On the other hand, we have already seen that they are in $\mathfrak{o}$. i.e. they are p -integral. It follows that they are rational integral. We thus have proved

LEMMA 3. *The matrix $(c_0^P)^{-1} \nabla_0' \bar{\nabla}_0$ is rational integral.*

The matrix $\nabla_0' \bar{\nabla}_0$ is positive-definite Hermitian. Indeed for any column y of complex numbers of length equal to the degree of $\nabla_0' \bar{\nabla}_0$, we have $y' \nabla_0' \bar{\nabla}_0 \bar{y} \geq 0$; if $y \neq 0$, then $\bar{\nabla}_0 \bar{y} \neq 0$ by the non-singularity of $\nabla_0' \bar{\nabla}_0$, and hence $y' \nabla_0' \bar{\nabla}_0 \bar{y} > 0$. We thus have

$$(23) \quad \det \nabla_0' \bar{\nabla}_0 > 0.$$

Consider now the product $\nabla_2' \bar{\nabla}_2$, where ∇_2 is as in (16). This

is also a non-negative hermitian matrix of the same degree. By

(4) we have

$$(24) \quad c_0^P = (\nabla_0' \nabla_2') \begin{pmatrix} \bar{\nabla}_0 \\ \bar{\nabla}_2 \end{pmatrix} = \nabla_0' \bar{\nabla}_0 + \nabla_2' \bar{\nabla}_2,$$

so that

$$(25) \quad \det c_0^P \geq \det \nabla_0' \bar{\nabla}_0,$$

the inequality sign holding if $\nabla_2' \bar{\nabla}_2 \neq 0$. 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 $W' C \bar{W} = I$, or

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

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

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

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

We now contend that $\nabla_2' \bar{\nabla}_2$ in fact vanishes. By Lemma 3. $\det \nabla_0' \bar{\nabla}_0$ is divisible by $\det c_0^P$ and since $\det \nabla_0' \bar{\nabla}_0$ is positive, $\det \nabla_0' \bar{\nabla}_0 \geq \det c_0^P$. However, by (25) we must have $\det \nabla_0' \bar{\nabla}_0 = \det c_0^P$, and this implies $\nabla_2' \bar{\nabla}_2 = 0$. This in turn evidently implies

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

§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*

$$(27) \quad \partial_{i\rho}^P = 0$$

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 χ_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*

$$(28) \quad \chi_i(PR) = 0$$

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 ϕ_ρ^P of $C(P)$. If $\tilde{B}$ is the block of $C(P)$ containing ϕ_ρ^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 χ is an irreducible character in a block of defect 0, then

$$(29) \quad \chi(G) = 0$$

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

$$(30) \quad \sum_{\chi_i \in B} \partial_{i\rho}^P \overline{\partial}_{i\sigma}^Q = 0$$

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

$$(31) \quad \sum_{\chi_i \in B} \partial_{i\rho}^P \overline{\partial}_{i\sigma}^P = \begin{cases} c_{\rho\sigma}^P & \text{if } \phi_\rho^P, \phi_\sigma^P \text{ belong to the same} \\ & \text{block } \tilde{B} \text{ of } C(P) \text{ and } \tilde{B}^G = B \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. We know by (4) that

$$(32) \quad \sum_{\tau=1}^t \sum_{\chi_i \in B_\tau} \partial_{i\rho}^P \overline{\partial}_{i\sigma}^Q = 0$$

where τ runs over the indices for the t blocks of G . If $\tilde{B}$ is the block of $C(P)$ containing ϕ_ρ^P , then $\partial_{i\rho}^P = 0$ for all χ_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 G , then*

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

for any block B of 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

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

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 G , where the $a_i \in \Omega$ and χ_i runs over all the irreducible characters of G . Then*

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

for any block B of 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 ρ runs over the indices of the irreducible modular characters of $C(P)$ and R_σ 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 ρ . 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 ρ , 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,

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

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 ψ 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 ψ 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

$$\psi(1) = \sum_{i \in B(p) \cap B'(q)} \chi_i(G) \chi_i(1) \equiv 0 \pmod{q^b}, \text{ which proves (35).}$$

We now return to consideration of blocks for a fixed prime p . For any p -element P and any block B_τ 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_τ ranges over all blocks of G , we have

$$\begin{aligned} \sum_{\tau=1}^t \ell_\tau(P) &= \text{number } \ell(P) \text{ of irreducible modular characters of} \\ &\quad C(P) \\ &= \text{number of } p\text{-regular conjugate classes of } C(P) \\ &= \text{number of conjugate classes of } G \text{ contained in the} \\ &\quad \text{section } S(P). \end{aligned}$$

Thus if $P_1=1, P_2, \dots, P_r$ 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_τ denotes the number of ordinary irreducible characters in B_τ .

PROPOSITION 4. *For every block B_τ of G*

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

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 χ_i is an irreducible character in B_τ , then by (1) and Theorem B, χ_i is a linear combination with coefficients $a_{i\sigma}^{P_\rho}$ 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 χ_i in B_τ is k_τ , we obtain

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

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

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 (ρ, τ) we define the $\ell_\tau(P_\rho) \times \ell(P_\rho)$ -matrix $\phi_{\rho, \tau}$, 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:

$\phi_{\rho, \tau} = (\phi_{\sigma}^{P_{\rho}}(R_{\alpha}^{P_{\rho}}))$, 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 $C(P_{\rho})$,

$\nabla_{\rho, \tau} = (\nabla_{i, \tau}^{P_{\rho}})$, 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 $\phi_{\rho, \tau}$.

Furthermore, set

$$\phi_{\tau} = \begin{pmatrix} \phi_{1, \tau} & & & 0 \\ & \phi_{2, \tau} & & \\ & \cdot & \cdot & \\ 0 & & & \phi_{r, \tau} \end{pmatrix}$$

$$\nabla_{\tau} = (\nabla_{1, \tau}, \nabla_{2, \tau}, \dots, \nabla_{r, \tau}),$$

$$X_{\tau} = (X_{1, \tau}, X_{2, \tau}, \dots, X_{r, \tau}).$$

In view of Theorem B, the relations (1), (5) may be written as

$$(37) \quad X_{\rho, \tau} = \nabla_{\rho, \tau} \phi_{\rho, \tau}$$

or

$$(38) \quad X_{\tau} = \nabla_{\tau} \phi_{\tau}.$$

Setting

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_t \end{pmatrix}, \quad \nabla = \begin{pmatrix} \nabla_1 & & 0 \\ & \cdot & \\ 0 & & \nabla_t \end{pmatrix}, \quad \phi = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_t \end{pmatrix},$$

we obtain

$$(39) \quad X = \nabla \phi.$$

Hence the matrices X , ∇ , and ϕ are all square matrices of degree $k = \sum_{\tau} k_{\tau}$. Furthermore, with a suitable arrangement of the rows, ϕ may be assumed decomposed into submatrices of the irreducible modular characters of $C(P_1)$, $C(P_2)$, $\dots$, $C(P_r)$. Hence $\det \phi \not\equiv 0 \pmod{p}$. Since p can be any prime factor of p in Ω , $\det \phi$ 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 Ω_0 be the field of g_0 -th roots of 1 over the rationals $\mathbb{Q}$, and let Ω_1 be the field of p^a -th roots of 1 over $\mathbb{Q}$. As before $(G:1) = g = p^a g_0$ with $(p, g_0) = 1$. Let σ be an element of the Galois group $\text{Gal}(\Omega_1/\mathbb{Q})$ of $\Omega_1/\mathbb{Q}$. σ may also be regarded as an element of $\text{Gal}(\Omega_1 \Omega_0/\Omega_0)$. Letting σ operate on (38), we obtain

$$(40) \quad X_{\tau}^{\sigma} = \nabla_{\tau}^{\sigma} \phi_{\tau}^{\sigma} = \nabla_{\tau}^{\sigma} \phi_{\tau},$$

since the values of the modular characters lie in Ω_0 by II, §2. It follows that if $\chi_i \in B_{\tau}$, then χ_i^{σ} also belongs to B_{τ} . Hence σ induces a permutation among the irreducible characters in B_{τ} . Accordingly, ∇_{τ}^{σ} is obtained from ∇_{τ} by a permutation of its rows, *i.e.*

$$(41) \quad \nabla_{\tau}^{\sigma} = U_{\tau}(\sigma) \nabla_{\tau}$$

for some permutation matrix $U_{\tau}(\sigma)$. On the other hand, there is a rational integer s prime to p such that each p^a -th root ϵ of 1 is sent by σ onto its s -th power ϵ^s . From (1) we then obtain

$$(42) \quad \chi_i^{\sigma}(P^s R) = \sum_{\rho} (\vartheta_{i\rho}^F)^{\sigma} \phi_{\rho}^P(R).$$

If P^s is conjugate to P_λ , and $P_\lambda = G^{-1}P^sG$ for some $G \in G$, then the map $T \rightarrow G^{-1}TG$ as T runs through $\mathcal{C}(P)$ gives an isomorphism of $\mathcal{C}(P) = \mathcal{C}(P^s)$ onto $\mathcal{C}(P_\lambda)$. Hence there is a permutation of the indices $\rho=1,2,\dots,\ell_\tau(P)=\ell_\tau(P_\lambda)$ such that

$$\phi_\rho^P(R) = \phi_\rho^{P_\lambda}(G^{-1}RG), \quad R \text{ } p\text{-regular in } \mathcal{C}(P).$$

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 ∇_τ^σ is obtained from ∇_τ by a permutation of its columns. If $V_\tau(\sigma)$ is the matrix of this permutation we thus have

$$(43) \quad \nabla_\tau^\sigma = \nabla_\tau V_\tau(\sigma).$$

Together with (41) we have

$$(44) \quad U_\tau(\sigma) \nabla_\tau = \nabla_\tau V_\tau(\sigma).$$

If σ_1 is a second element of $\text{Gal}(\Omega_1/Q)$, then we easily see from (41) and the non-singularity of ∇_τ 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 σ run over $\text{Gal}(\Omega_1/Q)$, we thus get two representations $\sigma \rightarrow U_\tau(\sigma)$ and $\sigma \rightarrow V_\tau(\sigma)$ of the abelian Galois group $\text{Gal}(\Omega_1/Q)$ by permutations; these are equivalent to each other by (44).

Let us call two ordinary irreducible characters χ_i, χ_j p-conjugate if there is an element σ of $\text{Gal}(\Omega_1\Omega_0/\Omega_0)$ (which is essentially the same as $\text{Gal}(\Omega_1/Q)$) 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_τ is equal to the number of families of algebraically conjugate columns of ∇_τ .*

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 Ω_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_τ and families of algebraically conjugate columns in ∇_τ such that corresponding families consist of the same number of members.*

PROOF. Since $p \neq 2$, $\text{Gal}(\Omega_1/Q)$ is cyclic. Let σ be a generator. The families of p-conjugate irreducible characters in B_τ 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 V_τ 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_τ there exist at least l_τ irreducible characters lying in Ω_0 .*

PROOF. Each of the l_τ columns of v_τ 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 l_τ irreducible characters χ_i in B_τ , each of which is p -conjugate to itself, i.e. lies in Ω_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. Curtis 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 Compact 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