J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On pseudo groups

Dedicated to Professor Shôkichi Iyanaga on his 60th Birthday

By Richard BRAUER

(Received June 14, 1967)

Introduction

An investigation of finite groups by means of group characters frequently leads to an array of numbers which looks like a perfectly reasonable table of characters. Actually there may exist groups G with these characters. On the other hand, it may turn out that no such groups exist.

It seems natural to study such arrays. Since they may be considered as generalizations of the system of group characters of finite groups, we will use the term *pseudo groups* for them. We shall see that they share some of the properties of groups. We require relatively little in our definition of pseudo groups in section 1. A stronger axiom is added in section 3. There are further conditions which one might impose. This is discussed briefly in the last section.

1. Definition of pseudo groups

We consider collections

(1.1) $$G=\{K, \Xi, v, E\}$$

where K is a finite set

(1.2) $$K=\{k_1, k_2, \cdots, k_r\},$$

Ξ is a set of complex-valued functions

(1.3) $$\Xi=\{\chi_1, \chi_2, \cdots . \chi_s\}$$

defined on K, v is a complex-valued function defined on K, and E is a set of mappings e_n of K into K, one for each rational integer n.

Each finite group G gives rise to a system (1.1), if the following interpretations are used:

(a) K is the set of conjugate classes of G.

(b) Ξ is the set of irreducible characters of G.

(c) If g is the order of G, then for each conjugate class k_j, $gv(k_j)$ is the number of elements in k_j.

(d) If σ is an element of the conjugate class k then $e_n(k)$ is the well defined conjugate class which contains σ^n.

We shall denote by $G(\mathfrak{G})$ the particular system (1.1) obtained in this manner from the given group $\mathfrak{G}$.

In the case of an arbitrary system (1), we shall use an analogous terminology. We call the element k_j the *classes*, even though they need not be sets of elements. The functions χ_i will be termed the *irreducible characters* of G. By a *character* χ of G, we mean a linear combination

$$\chi = \sum_j a_j \chi_j \tag{1.4}$$

with non-negative rational integral a_j.

It will be convenient to write k^n for $e_n(k)$.

If $\tilde{G} = \{\tilde{K}, \tilde{\Xi}, \tilde{v}, \tilde{E}\}$ is a second system, a mapping ζ of $\tilde{K}$ into K will be called an *imbedding* of $\tilde{G}$ into G, if the following conditions are satisfied:

(α) If χ is an irreducible character of G, the composite function $\chi \circ \zeta$ is a character of $\tilde{G}$.

(β) $\zeta \circ \tilde{e}_n = e_n \circ \zeta$.

(γ) If $\zeta(\tilde{k}^n) = \zeta(\tilde{k}^0)$ for some $\tilde{k} \in \tilde{K}$, then $\tilde{k}^n = \tilde{k}^0$.

If $\tilde{\mathfrak{G}}$ is a subgroup of a group $\mathfrak{G}$, we have a natural imbedding of $G(\tilde{\mathfrak{G}})$ into $G(\mathfrak{G})$.

We shall call the system G in (1) a *pseudo-group*, if the following axioms are satisfied:

(I) The number s of irreducible characters χ_i is equal to the number r of classes k_j[1]. The functions $\chi_1, \cdots, \chi_r$ satisfy the "orthogonality relations"

$$\sum_{k \in K} v(k) \chi_i(k) \overline{\chi}_j(k) = \delta_{ij} \tag{1.5}$$

for $i, j = 1, 2, \cdots, r$.

(II) The product of two irreducible characters χ_i, χ_j of G is a character of G.

(III) The constant 1 is an irreducible character of G.

(IV) There is a fixed class denoted by 1 such that $k^0 = 1$ for each $k \in K$.

(V) For each class k, there exists a positive integer m such that the system $G(\mathfrak{Z}_m)$ belonging to a cyclic group $\mathfrak{Z}_m = \langle \sigma \rangle$ of order m have imbeddings ζ into G with $\zeta(\sigma) = k$.

Obviously, m is uniquely determined by k. We call m the *order* of k.

(VI) If k is a class of order m and if m and the integer n are coprime, then $v(k) = v(k^n)$.

It is clear that if $\mathfrak{G}$ is a group, $G(\mathfrak{G})$ is a pseudo-group.

If k is a class of order m, it follows from (V) that m is the first positive

1) It suffices to require $s \geqq r$.

integer for which $k^m=1$. We have $k^1=k$, $(k^q)^n=k^{qn}$. We may have $k^n=k^q$ for $0<n<q<m$.

By $A=A(G)$, we denote the algebra of all complex-valued functions defined on K. For two such *class functions* $\varphi, \psi \in A$, we define an inner product

$$(\varphi, \psi)=\sum_{k\in K} v(k)\varphi(k)\overline{\psi(k)}.$$

Then $\{\chi_1, \cdots, \chi_r\}$ is an orthonormal basis of A, cf. (1.5).

By a *generalized character* of G, we mean a difference of two characters. It follows from (II) that the generalized characters form a ring. An element $\varphi\in A$ is a generalized character, if and only if the product (φ, χ_j) belongs to the ring $\boldsymbol{Z}$ of integers for $j=1, 2, \cdots, r$. The element φ is a character, if and only if all (φ, χ_j) are non-negative elements of $\boldsymbol{Z}$.

Let (χ) denote the $(r\times r)$-matrix $(\chi_i(k_j))$ with i as row-index and j as column index. If V is the diagonal matrix with the entry $v(k_i)$ in the i-th row, then (1.5) can be written in the form

$$(\chi)V(\overline{\chi})^T=I^{2)}. \tag{1.6}$$

It follows that $v(k_i)\neq 0$ for each i. We set

$$c(k_i)=v(k_i)^{-1}. \tag{1.7}$$

In the following, we shall work with the function c rather than with the function v. If several pseudo-groups occur, we shall write c_G instead of c. In particular, $c(1)$ will be called the *order* of G. Since (6) implies

$$(\overline{\chi})^T(\chi)=V^{-1},$$

we have the orthogonality relation of second kind

$$\sum_{\chi\in\Xi}\overline{\chi}(k_i)\chi(k_j)=c(k_i)\delta_{ij}, \tag{1.8}$$

$(1\leqq i, j\leqq r)$. As indicated, χ here ranges over all irreducible characters of G.

Consider a fixed class k of order m and let ζ denote the imbedding of the system $G(\mathfrak{Z}_m)$ given by Axiom (V): Clearly, ζ is unique. Let $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m\}$ denote the m-th roots of unity. If χ is a character of G, the condition (α) for imbeddings implies that $\chi\circ\zeta$ is a character of the cyclic group $\mathfrak{Z}_m$. It follows that

$$\chi(k^i)=\sum_{j=0}^{m-1} b_j\varepsilon_j^i \tag{1.9}$$

where the b_j are non-negative integers which depend on k but not on i. This shows that all $\chi(k^i)$ lie in the field Ω_m of the m-th roots of unity. If σ is an element of the Galois group of Ω_m over the field $\boldsymbol{Q}$ of rational numbers and

2) The transpose of a matrix M is denoted by M^T and $\overline{M}^T$ is the conjugate complex of M^T.

if σ maps a primitive m-th root of unity ε on ε^n with $n \in \boldsymbol{Z}$, $(m, n)=1$, then

$$\chi(k)^{\sigma}=\chi(k^n)\,. \tag{1.10}$$

In particular,

$$\overline{\chi(k)}=\chi(k^{-1})\,. \tag{1.11}$$

It is also clear from (1.9) that the *degree* $\chi(1)$ of the character χ is a non-negative rational integer

$$\chi(1)=\sum_{j=0}^{m-1} b_j\;; \tag{1.12}$$

we have $\chi(1)=0$ if and only if $\chi=0$.

By (1.8), $c(k)$ is an algebraic integer and, if k has order m, then $c(k)\in \Omega_m$. It now follows from (1.10), (1.7) and Axiom VI that $c(k)$ is a rational integer. Clearly, $c(k)>0$. In particular, we have

(1A) *The order of a pseudo-group is a positive rational integer g.*

It follows from (1.9) and (1.12) that, for each class k, we have $|\chi(k)|\leqq \chi(1)$. Then (1.8) implies that $c(k)\leqq g$.

2. Sub-pseudo-groups

Consider two pseudo-groups

$$G=\{K, \Xi, 1/c, E\}\,, \qquad \tilde{G}=\{\tilde{K}, \tilde{\Xi}, 1/\tilde{c}, \tilde{E}\}$$

where we now expressed the weight-function v by its reciprocal c, cf. (1.7). If ζ is an imbedding of $\tilde{G}$ into G, we say that the pair $(\tilde{G}, \zeta)$ is a *sub-pseudo-group* of G. There may exist distinct imbeddings ζ, ζ_1 of $\tilde{G}$ into G. Then $(\tilde{G}, \zeta)$ and $(\tilde{G}, \zeta_1)$ will be considered as distinct sub-pseudo-groups.

If $(\tilde{G}, \zeta)$ is a sub-pseudo-group of G, and (H, η) a sub-pseudo-group of $\tilde{G}$, then $(H, \zeta\circ\eta)$ is a sub-pseudo-group of G.

If $\mathfrak{G}$ is a group and $\tilde{\mathfrak{G}}$ a subgroup, we have a natural imbedding of $G(\tilde{\mathfrak{G}})$ into $G(\mathfrak{G})$. Obviously, conjugate subgroups define the same sub-pseudo-group.

Let G and $\tilde{G}$ be pseudo-groups and let $(\tilde{G}, \zeta)$ be a sub-pseudo-group of G. If $\theta \in A(G)$ is a class function of G, we can define a class function θ_ζ on H by setting

$$\theta_\zeta=\theta\circ\zeta\,. \tag{2.1}$$

Clearly, the mapping $\theta\to\theta_\zeta$ is a linear mapping of $A(G)$ into $A(\tilde{G})$. In the case of groups, this is the restriction map and the conjugate map of $A(\tilde{G})\to A(G)$ maps each class function $\varphi\in A(\tilde{G})$ on the function $\varphi^\zeta\in A(G)$ "induced" by φ. This carries over to the case of a pseudo-group G and a sub-pseudo-group $(\tilde{G}, \zeta)$. If k is a class of G, we set

$$\varphi^{\zeta}(k)=c(k)\sum_{l\in\zeta^{-1}(k)}\tilde{c}(l)^{-1}\varphi(l) \tag{2.2}$$

where the sum on the right extends over all classes $l\in\tilde{K}$ of $\tilde{G}$ for which $\zeta(l)=k$. Just as in the group case, one sees that, for $\theta\in A(G)$, $\varphi\in A(\tilde{G})$, we have

$$\varphi^{\zeta}\cdot\theta=(\varphi\cdot\theta_{\zeta})^{\zeta}, \tag{2.3}$$

and the "Frobenius reciprocity"

$$(\varphi^{\zeta},\theta)=(\varphi,\theta_{\zeta}). \tag{2.4}$$

The usual proof then yields.

(2A) Let G and $\tilde{G}$ be pseudo-groups and let $(\tilde{G},\zeta)$ be a sub-pseudo-group of G. If ψ is a character of $\tilde{G}$, then ψ^{ζ} is a character of G.

If G and $\tilde{G}$ have orders g and $\tilde{g}$ respectively,

$$\tilde{g}\cdot\psi^{\zeta}(1)=g\psi(1). \tag{2.5}$$

As a corollary, we note

(2B) *The order $\tilde{g}$ of a sub-pseudo-group $(\tilde{G},\zeta)$ of the pseudo group G divides the order g of G.*

Indeed, we see this when we take ψ as the constant 1 in (2.5). We use the ordinary notation $|G:\tilde{G}|$ for $g/\tilde{g}$ and speak of the *index* of $\tilde{G}$ in G. We see in the same manner that for each class k of G,

$$c(k)\sum_{l\in\zeta^{-1}(k)}\tilde{c}(l)^{-1}\in\boldsymbol{Z}, \tag{2.6}$$

where $\boldsymbol{Z}$ denotes the ring of rational integers.

It follows from (2B) and Axiom V that the order m of each class k of a pseudo-group G divides the order g of G. The *exponent* e of G can be defined as the least common multiple of the orders of the classes k of G. Then e divides the order g of G.

The following statement is obvious on account of the results of Section 1.

(2C) *Let G be a pseudo-group of exponent e. The values of the characters of G lie in the field of the e-th roots of unity.*

It will be clear what we mean by an isomorphism of pseudo-groups.

(2D) *Assume that $(\tilde{G},\zeta)$ is a sub-pseudo-group of the pseudo-group G and that G and $\tilde{G}$ have the same order $g=\tilde{g}$. Then ζ defines an isomorphism of $\tilde{G}$ onto G.*

PROOF. If $\tilde{\chi}_i$ is an irreducible character of $\tilde{G}$, then by (2A), $\tilde{\chi}_i^{\zeta}$ is a character of G of the same degree as $\tilde{\chi}_i$. If χ_j is an irreducible constituent of $\tilde{\chi}_i^{\zeta}$, by the Frobenius reciprocity law (2.4), $\tilde{\chi}_i$ is an irreducible constituent of $(\chi_j)_{\zeta}$. It follows that $\tilde{\chi}_i(1)=\chi_j(1)$ and hence that $\tilde{\chi}_i^{\zeta}=\chi_j$, $(\chi_j)_{\zeta}=\chi_i$. Each irreducible character χ_j of G can be obtained in the form $\tilde{\chi}_i^{\zeta}$ and ζ establishes a one-to-one mapping of the set $\tilde{\Xi}$ of irreducible characters of $\tilde{G}$ onto the corresponding set Ξ for G.

The mapping ζ maps the set $\tilde{K}$ of classes of G into the set K of classes of G. If $\zeta(\tilde{K})\neq K$, choose $k\in K$, $k\notin\zeta(\tilde{K})$. Then

$$\tilde{\chi}_i^{\zeta}(k)=0$$

for each $\tilde{\chi}_i\in\tilde{\Xi}$. But then $\chi_j(k)=0$ for each $\chi_j\in\Xi$ and this is certainly false. Since $\tilde{G}$ and G have the same number of classes, ζ is a one-to-one mapping of $\tilde{K}$ onto K. By (1.8), $\tilde{c}(\tilde{k})=c(\zeta(\tilde{k}))$ for all classes $\tilde{k}$ of $\tilde{G}$. Finally,

$$\zeta\circ\tilde{e}_n=e_n\circ\zeta$$

by the condition (β) in the definition of imbedding. This proves (2D).

(2E) Let $(\tilde{G},\zeta)$ be a sub-pseudo-group of the pseudo-group G. Assume that ζ maps the set $\tilde{K}$ of classes of $\tilde{G}$ onto the set of classes K of G. Then G and $\tilde{G}$ have the same order and ζ establishes an isomorphism of $\tilde{G}$ onto G.

PROOF. If we use the same notation as before, then (2.6) can be written in the form

$$\sum_{l\in\zeta^{-1}(k)}\tilde{v}(l)=M(k)v(k) \tag{2.7}$$

with $M(k)\in\boldsymbol{Z}$, cf. (1.7). Moreover, $M(k)>0$.

Applying (1.5) to $\chi_i=\chi_j=1$, we have

$$\sum_{k\in K}v(k)=1\,,\qquad \sum_{l\in\tilde{K}}\tilde{v}(l)=1\,,$$

and (2.7) yields

$$M(k)=\sum_{k\in K}M(k)v(k)\leqq\sum_{l\in\tilde{K}}\tilde{v}(l)=1\,.$$

Thus, $M(k)=1$ for all classes. In particular, for $k=1$, we have $v(1)=\tilde{v}(1)$ and hence $g=\tilde{g}$. Now, (2C) applies and yields the statement.

In the group case, (2E) yields the well known result that if a subgroup $\tilde{G}$ of a group G meets every conjugate class of G, then $G=\tilde{G}$.

3. Artin's Theorem

By a *cyclic subgroup* of a pseudo-group G, we mean a sub-pseudo-group $(\tilde{G},\zeta)$ with $\tilde{G}$ of the form $G(Z)$, Z a cyclic group.

We can state Artin's theorem in the form

(3A) *Let G be a pseudo-group. Let n be the least common multiple of the numbers $c(k)$ for the classes k of G. If χ is a character of G, then χ can be written in the form*

$$\chi=\frac{1}{n}\sum_j c_j\phi_j \tag{3.1}$$

where each ϕ_j is a character of G induced by a character of a cyclic subgroup *and where the c_j are rational integers.*

The proof does not differ substantially from a proof in the group case and we sketch it only briefly. Let e be the exponent of G and let ε be a primitive e-th root of unity. Set $R=\boldsymbol{Z}[\varepsilon]$. It will suffice to prove that χ can be written in the form (3.1) with $c_j \in R$. If we then express each c_j by a $\boldsymbol{Z}$-basis $\omega_1=1,\ \omega_2, \cdots$ of R, the method in [**1**] yields a representation of χ with coefficients c_j in $\boldsymbol{Z}$.

Let V_R denote the set of all linear combinations

$$\sum_j b_j \psi_j$$

where each ψ_j is a character of G induced by a character of a cyclic subgroup of G and where the coefficients b_j belong to R. We have to show that $n\chi$ belongs to V_R.

Let h be a fixed class, say of order m, set $\tilde{G}=G(\mathfrak{Z}_m)$ and let ζ denote the imbedding of $\tilde{G}$ into G given by Axiom V which maps the generator σ of $\mathfrak{Z}_m$ on h. Define a class function ψ on $G(\mathfrak{Z}_m)$ by setting

$$\psi(\sigma)=m\,, \qquad \psi(\sigma^j)=0 \qquad \text{for} \quad \sigma^j \neq \sigma\,.$$

Let η_h denote the induced function on G. Then

$$\eta_h(k)=c(k)\sum_{l\in\zeta^{-1}(k)} m^{-1}\psi(l)=\begin{cases} c(h) & \text{for} \quad k=h\,,\\ 0 & \text{for} \quad k\neq h\,.\end{cases}$$

As ψ is a linear combination of characters of $G(\mathfrak{Z}_m)$ with coefficients in R, we have $\eta_h \in V_R$ for each class h of G.

On the other hand, we can set

$$\chi=\sum_{h\in K}\chi(h)c(h)^{-1}\eta_h\,.$$

Since all $nc(h)^{-1}\chi(h)$ lie in R, we have $n\chi \in V_R$ and the proof is complete.

4. Characterization of characters

Our next aim is to establish the results of [**1**] for pseudo-groups. This seems to require an additional axiom. We begin with some definitions. In them, p will be a fixed prime number. If k is a class of order m of a pseudo-group and if $m=p^a b$ with $(p, b)=1$, we determine u and v in $\boldsymbol{Z}$ such that

$$1=u+v\,, \qquad u\equiv 0 \pmod{p^a}, \qquad v\equiv 0 \pmod{b}\,.$$

Then

$$\mathfrak{R}(k)=k^u\,, \qquad \mathfrak{S}(k)=k^v$$

are uniquely determined by k. We call $\mathfrak{R}(k)$ the *p-regular factor* and $\mathfrak{S}(k)$ the *p-singular* factor of k. The class k is *p-regular*, if its order is prime to p.

Then $\mathfrak{R}(k)=k$. For each k, $\mathfrak{R}(k)$ is p-regular.

DEFINITION. Let H be a pseudo-group, let p be a prime number. We call H a *p-elementary* pseudo-group with the *base factor h*, if the following conditions are satisfied.

(*a*) The class h is p-regular. If its order is m, the classes

$$1, h, h^2, \cdots, h^{m-1}$$

are distinct and they are the only p-regular classes of H.

(*b*) Let $(G(\mathfrak{Z}_m), \zeta)$ be a cyclic subgroup of G such that ζ maps the generator σ of $\mathfrak{Z}_m$ on h, (cf. Axiom V). If ω is an irreducible character of $\mathfrak{Z}_m$ then

$$\phi(k)=\omega\zeta^{-1}(\mathfrak{R}(k)), \qquad (k \in K)$$

is a character of G.

A pseudo-group will be said to be *elementary*, if it is p-elementary for a suitable prime p.

If $\mathfrak{G}$ is a direct product of a p-group and a group of order prime to p, then $G(\mathfrak{G})$ is p-elementary.

Our additional axiom is:

AXIOM (A). Let G be a pseudo-group. Let p be an arbitrary prime. If k is a p-regular class of G, there exists a sub-pseudo group (H, ζ) such that H is p-elementary with the base factor h, that $\zeta(h)=k$, and that the following condition holds: The prime p divides $c_H(h)$ at least with the same exponent with which p divides $c_G(k)$.

In the case of group systems $G(\mathfrak{G})$, $c_G(k)$ is the order of the centralizers $\mathfrak{C}_{\mathfrak{G}}(\tau)$ for elements τ in the conjugate class k. If $\mathfrak{P}$ is a p-Sylow sub-group, if we set $\mathfrak{H}=\langle\tau\rangle\times\mathfrak{P}$ and $H=G(\mathfrak{H})$, we see immediately that the Axiom (A) holds in $G(\mathfrak{G})$.

Now the methods of [**1**] can be applied. They yield the following two equivalent statements.

(4A) *Let G be a pseudo-group for which Axiom* (A) *is satisfied. The following condition is necessary and sufficient in order that a class function θ on G be a generalized character: If (H, ζ) is an elementary sub-pseudo-group of G, then θ_ζ is a generalized character of H.*

(4B) *Each character χ of G in* (4A) *can be written in the form*

$$\chi=\sum c_i\phi_i$$

where each ϕ_i is a character of G induced by a character of an elementary sub-pseudo-group (H, ζ) of G and where $c_i \in \boldsymbol{Z}$.

A class function θ on G is an irreducible character of G, if and only if in addition to the condition in (4A), the following conditions hold

$$(\theta, \theta)=1, \qquad \theta(1)>0.$$

5. Additional remarks

We are mainly interested in pseudo-groups $G(\mathfrak{G})$ belonging to groups $\mathfrak{G}$. In this case, a number of further properties of classes and characters are known. In principle, each of them could be introduced as a new axiom. We mention only a few possibilities.

AXIOM B. Let k, h, l be classes of a pseudo-group G of order g. Then

$$a(k, h, l)=gc(k)^{-1}c(h)^{-1}\sum_{i}\chi_i(k)\chi_i(h)\overline{\chi_i(l)}\chi_i(1)^{-1}$$

(the sum extended over all irreducible characters of G) is a non-negative rational integer.

If this is so, we can define a commutative and associative algebra T whose elements are formal linear combinations

$$\sum_{k\in K} u_k k$$

with coefficients $u_k \in \boldsymbol{Z}$. Multiplication is defined by means of

$$k\cdot h=\sum_{l\in K} a(k, h, l)\, l\,.$$

In the case of group systems $G(\mathfrak{G})$, T will be the class algebra of G.

If the Axiom (B) holds, the usual proof shows that, for each irreducible character χ_i of G and each class k, the number

$$gc(k)^{-1}\chi_i(k)\chi_i(1)^{-1}$$

is an algebraic integer. It follows that the degrees of the irreducible characters divide g. It is also clear that $c(k)$ must divide g. The number n in (3A) then is equal to g (as in the usual form of Artin's theorem).

AXIOM (C). Let χ_i be a character of degree x of a pseudo-group G. Let Y be one of the Schur representations of the general linear group $GL(x, \boldsymbol{C})$, and η its character, cf. [2], [3]. Then η applied to χ in the obvious manner yields a character of G.

This can be modified in various ways.

Other possible axioms might describe other known group theoretical statements. For instance, we may require that $c(k)$ is the order of a sub-pseudo-group $(C(k), \zeta)$ of a particular type. Our aim then would be to replace axiom (A) in Section IV. However, it seems that further postulates are needed.

We may also incorporate results of the theory of modular characters as axioms.

As is well known if $\mathfrak{G}$ is a group, it can be seen from the table of characters whether or not $\mathfrak{G}$ is simple. An analogous condition is to define *simplicity* of pseudo-groups.

It will be clear that a great number of questions arise. Many of them seem to be very difficult. Of course, if one could describe all simple pseudo-groups, this would have far reaching effects on the theory of simple groups. In some ways, the algebraic conditions characterizing simple pseudo-groups may seem simpler than the conditions for simple groups. (At least, they might look simpler to a computer.) On the other hand, in discussing pseudo-groups, we cannot use many of the powerful methods of group theory.

It might be of some interest to study simple pseudo-groups in which all the quantities depend in a well-specified manner on a parameter q.

Harvard University

References

[1] R. Brauer and J. Tate, On the characters of finite groups, Ann. of Math., 62 (1955), 1–7.

[2] I. Schur, Ueber eine Klasse von Matrizen, die sich einer gegebenen Matrix zuordnen lassen, Dissertation, Berlin, 1901.

[3] H. Weyl, The classical groups, Princeton University Press, 1946.