On projective representations and ring extensions of finite groups

By Keijiro YAMAZAKI

Dedicated to Professor Masao SUGAWARA

Contents

Introduction.

The theory of projective representations (Darstellungen durch gebrochene lineare Substitutionen) of finite groups over the complex number field was founded and developed by I. Schur [1], [2], [3]. Schur [1] reduced the problem to determine all projective representations of a finite group $\mathfrak{H}$ to the determination of all linear representations of a certain finite group extension $\mathfrak{G}$ of $\mathfrak{H}$, which is called a representation-group of $\mathfrak{H}$. Also Schur [2] gave an estimation for the number of non-isomorphic representation-groups. In [2] and [3], Schur determined all irreducible projective representations of $\mathfrak{S}_n$, $\mathfrak{A}_n$, $\mathrm{PGL}(2, \mathrm{F}_q)$, $\mathrm{SL}(2, \mathrm{F}_q)$ and $\mathrm{PSL}(2, \mathrm{F}_q)$.

Then R. Frucht [4], [13] determined the irreducible projective representations of finite abelian groups. For other basic fields, see K. Asano [5], K. Asano-K. Shoda [7], K. Asano - M. Osima - M. Takahasi [9]. See also Y. Kawada [10] and G. W. Mackey [14] for the projective representations of topological groups.

In this note, we shall give in §1 the fundamental concepts of projective representations as preliminaries. We observe that the transgression $\mathrm{H}^1(\mathfrak{A}, \Omega) \to \mathrm{H}^2(\mathfrak{H}, \Omega)$ by G. Hochschild and J.-P. Serre [12] is essentially the same as the mapping given by Schur when $\Omega = \mathrm{C}^*$. (Note also that the method of Schur to find the "multiplier" $\mathrm{H}^2(\mathfrak{H}, \mathrm{C}^*)$ using a representation-group is nothing but the method given in S. Eilenberg - S. MacLane [11] using the cup product reduction.)

In §2, we consider some useful relations between 2-cocycles and pairings. Then 2-cohomology, for the trivial action on a coefficient group, of a finitely generated abelian group is explicitly determined.

§3 is concerned with a cohomology theoretical consideration of various central group extensions of a finite group. A fundamental exact sequence will imply the existence of representation-groups and yield Schur's estimation for the number of these groups. It should be noted that the method used in this section is somewhat related to [7].

When the basic field is not algebraically closed, the multiplier is not necessarily finite; we have thereby no finite representation-group. In this case, the concept of ring extension will play a role of "linearization" of projective representations (§4, §5). The concept of "crossed product" is nothing but a ring extension under the faithful action. We shall call "algebra extension" a ring extension under the trivial action. This is a generalization of group algebra (Cf. [6], [7], [9]). We shall take some automorphisms of an algebra extension and show that it is necessary to consider an equivalence of modules w.r.t. these automorphisms.

In §6, we shall determine the structure of algebra extensions of a finite abelian group over a field of some type. A result of Frucht [4] on projective representations is reproduced and generalized without any use of representation-groups. Moreover, we get a necessary and sufficient condition for the existence of central simple algebra extensions of a finite abelian group. Those algebras are closely related to faithful irreducible projective representations.

§ 7 is devoted to several applications. There are various representation-groups of a finite group, e.g. the multipliers of these groups are in general different (Cf. N. Iwahori - H. Matsumoto [15]). However it can be proved that the group algebras of all representation-groups of a finite group are isomorphic as algebra. We see that the total matric algebras and the Kummer fields are typical examples of algebra extensions of abelian groups. Also it is seen that the Clifford algebras are algebra extensions of a special type. In addition, we shall give a remark on algebra extensions of non-abelian groups (Cf. also [15]).

The author will conclude this introduction by acknowledging his thanks to Prof. N. Iwahori for many suggestions and discussions, and referring to Iwahori-Matsumoto [15].

§ 1. Preliminaries.

1.1. Cohomology groups of a group.

Let us recall the definition of cohomology groups of any group $\mathfrak{H}$ which acts on an abelian group Ω.[1] (Cf. S. Eilenberg - S. MacLane [11]) For later use Ω is written multiplicatively.

A function f of n variables defined on $\mathfrak{H}$ and with values in Ω is called an *n-cochain* of $\mathfrak{H}$ in Ω ($n=0, 1, 2, \cdots$).[2] The set of all n-cochains becomes an abelian group $\mathrm{C}^n(\mathfrak{H}, \Omega)$ under the multiplication of values. The *coboundary* of an n-cochain f is defined to be the $(n+1)$-cochain δf, where

$$\begin{aligned}&(\delta f)(P_1, \cdots, P_{n+1})\\ &={}^{P_1}f(P_2, \cdots, P_{n+1})\prod_{i=1}^{n} f(P_1, \cdots, P_iP_{i+1}, \cdots, P_{n+1})^{(-1)^i} f(P_1, \cdots, P_n)^{(-1)^{n+1}}.\end{aligned}$$

It is easily verified that (Cf. [11])

$$\delta(fg)=(\delta f)(\delta g), \quad \delta(\delta f)=1.^{3)} \tag{1}$$

The set $\mathrm{Z}^n(\mathfrak{H}, \Omega)$ of all *n-cocycles* f, for which $\delta f=1$, constitutes a subgroup of $\mathrm{C}^n(\mathfrak{H}, \Omega)$. The set $\mathrm{B}^n(\mathfrak{H}, \Omega)$ of all n-coboundaries constitutes a subgroup of

1) This means that for each $H\in\mathfrak{H}$ and $\lambda\in\Omega$ there is determined an element ${}^H\lambda\in\Omega$ such that ${}^H(\lambda\mu)={}^H\lambda{}^H\mu$, ${}^{(PQ)}\lambda={}^P({}^Q\lambda)$ and ${}^I\lambda=\lambda$ (I is the unit element of $\mathfrak{H}$).

2) A 0-cochain means an element of Ω.

3) We denote by 1 the function taking the constant value 1.

$Z^n(\mathfrak{H}, \Omega)$.[4] The *n-cohomology group* is defined to be

$$H^n(\mathfrak{H}, \Omega)=Z^n(\mathfrak{H}, \Omega)/B^n(\mathfrak{H}, \Omega),$$

and its element is called a *cohomology class*. Any two cocycles contained in the same cohomology class are called to be *cohomologous*.

An n-cochain f is said to be *normalized* if $f(P_1, \cdots, P_n)=1$ whenever any one of the P_i is the unit element of $\mathfrak{H}$. It can be proved that every cocycle is cohomologous to a normalized cocycle. A 1-cocycle is always normalized. For a 2-cocycle f, if we define a 1-cochain g where

$$g(P)=\begin{cases} f(I, I)^{-1} & P=I, \\ 1 & \text{otherwise}, \end{cases}$$

then $f(\delta g)$ is normalized. Using only normalized cochains, cocycles and coboundaries, we get isomorphic cohomology groups (Cf. [11]).

Now let Ω_1 and Ω_2 be abelian groups on which $\mathfrak{H}$ acts and φ be a $\mathfrak{H}$-homomorphism of Ω_1 into Ω_2. Then φ induces a homomorphism $\bar{\varphi}: H^n(\mathfrak{H}, \Omega_1)\rightarrow H^n(\mathfrak{H}, \Omega_2)$ naturally. If

$$1\rightarrow\Omega'\rightarrow\Omega\rightarrow\Omega''\rightarrow 1 \tag{2}$$

is an exact sequence, the we have clearly the exact sequence which is compatible with δ:

$$1\rightarrow C^n(\mathfrak{H}, \Omega')\rightarrow C^n(\mathfrak{H}, \Omega)\rightarrow C^n(\mathfrak{H}, \Omega'')\rightarrow 1 \qquad (n\geqq 0)$$

We easily see using only the property (1) that the following exact sequence is naturally induced as usual topology.

$$\begin{aligned} &H^0(\mathfrak{H}, \Omega')\rightarrow H^0(\mathfrak{H}, \Omega)\rightarrow H^0(\mathfrak{H}, \Omega'')\rightarrow H^1(\mathfrak{H}, \Omega')\rightarrow H^1(\mathfrak{H}, \Omega)\rightarrow H^1(\mathfrak{H}, \Omega'') \\ &\rightarrow H^2(\mathfrak{H}, \Omega')\rightarrow H^2(\mathfrak{H}, \Omega)\rightarrow H^2(\mathfrak{H}, \Omega'')\rightarrow H^3(\mathfrak{H}, \Omega')\rightarrow H^3(\mathfrak{H}, \Omega)\rightarrow\cdots \end{aligned} \tag{3}$$

In particular, if (2) splits, then we have the splitting exact sequence

$$1\rightarrow H^n(\mathfrak{H}, \Omega')\rightarrow H^n(\mathfrak{H}, \Omega)\rightarrow H^n(\mathfrak{H}, \Omega'')\rightarrow 1 \qquad (n>0). \tag{4}$$

Let Ω be any abelian group and d a positive integer. We consider the homomorphism φ of Ω into itself by $\varphi(\lambda)=\lambda^d$. We shall denote by Ω^d the image of this homomorphism and by $\Omega_{(d)}$ the kernel. If $\Omega^d=\Omega$, Ω is called to be *d-divisible*. The following proposition will be used later.

PROPOSITION 1.1. *Let $\mathfrak{H}$ be a group acting on an abelian group Ω.*

1) *If $\mathfrak{H}$ is a finite group of order h, then we have*

$$H^n(\mathfrak{H}, \Omega)=H^n(\mathfrak{H}, \Omega)_{(h)} \qquad (n>0).$$

4) $B^n(\mathfrak{H}, \Omega)=\{1\}$.

2) *If Ω is d-divisible, then we have the surjective homomorphism*

$$\mathrm{H}^n(\mathfrak{H}, \Omega_{(d)}) \to \mathrm{H}^n(\mathfrak{H}, \Omega)_{(d)} \qquad (n \geqq 0)$$

induced by the natural injection $\Omega_d \to \Omega$.

PROOF. 1) We assume $n=2$, but the following computation[5] is also valid for any $n>0$. Let $f \in \mathrm{Z}^2(\mathfrak{H}, \Omega)$. We have

$$1=(\delta f)(P, Q, R)={}^P f(Q, R) f(PQ, R)^{-1} f(P, QR) f(P, Q)^{-1}$$

for $P, Q, R \in \mathfrak{H}$. We define $g \in \mathrm{C}^1(\mathfrak{H}, \Omega)$ by

$$g(H)=\prod_{P \in \mathfrak{H}} f(H, P) \qquad \text{for } H \in \mathfrak{H}.$$

Then it follows easily that $f^h=\delta g$. This completes the proof of 1).

2) By the assumption, we have the exact sequence

$$1 \to \Omega_{(d)} \to \Omega \xrightarrow{\varphi} \Omega \to 1$$

where $\varphi(\lambda)=\lambda^d$. This yields the following exact sequence.

$$\mathrm{H}^n(\mathfrak{H}, \Omega_{(d)}) \to \mathrm{H}^n(\mathfrak{H}, \Omega) \xrightarrow{\bar{\varphi}} \mathrm{H}^n(\mathfrak{H}, \Omega) \qquad (n \geqq 0)$$

where $\bar{\varphi}(c)=c^d$ ($c \in \mathrm{H}^n(\mathfrak{H}, \Omega)$). This completes the proof of 2).

1.2. Projective representations of a group.

Let $\mathfrak{H}$ be a group and V be a finite dimensional vector space over a field K. The group of all automorphisms of V is denoted by $\mathrm{GL}(V)$. The center of $\mathrm{GL}(V)$ is equal to K^*1_V, where $K^*=K-\{0\}$ and 1_V denotes the identity mapping of V onto itself. The factor group $\mathrm{GL}(V)/K^*1_V$ is denoted by $\mathrm{PGL}(V)$. This is the group of projective transformations of the projective space $\mathrm{P}(V)$ associated to V.

A homomorphism $\rho: \mathfrak{H} \to \mathrm{PGL}(V)$ is called a *projective representation* of $\mathfrak{H}$ in V. $n=\dim_K V$ is called the *degree* of ρ and V is called the *representation space* of ρ. Two projective representations $\rho_i: \mathfrak{H} \to \mathrm{PGL}(V_i)$ $(i=1, 2)$ are called to be *equivalent* (in notation: $\rho_1 \sim \rho_2$) if there exists a linear isomorphism $\varphi: V_1 \to V_2$ such that $\tilde{\varphi} \circ \rho_1=\rho_2$ where $\tilde{\varphi}$ is the isomorphism $\mathrm{PGL}(V_1) \to \mathrm{PGL}(V_2)$ which is induced by the isomorphism $\mathrm{GL}(V_1) \to \mathrm{GL}(V_2): \tau \to \varphi\tau\varphi^{-1}$ $(\tau \in \mathrm{GL}(V_1))$.

Let ρ be a projective representation of $\mathfrak{H}$ in V and ρ_1 be a projective representation of $\mathfrak{H}$ in a subspace V_1 of V such that $\rho_1(H)$ is the restriction of $\rho(H)$ to $\mathrm{P}(V_1)$ for all $H \in \mathfrak{H}$. Then ρ_1 is called a *subrepresentation* of ρ. ρ is called to be *irreducible* if there is no proper subrepresentation of ρ, that is, there is no proper $\pi^{-1}(\rho(\mathfrak{H}))$-invariant subspace of V where π is the natural projection of $\mathrm{GL}(V)$ onto $\mathrm{PGL}(V)$.

5) This was given by Schur [1].

A mapping $T:\mathfrak{H}\to \mathrm{GL}(V)$ is called a *section* for ρ if $\pi(T(H))=\rho(H)$ for any $H\in\mathfrak{H}$. Any section T for ρ defines a mapping $f:\mathfrak{H}\times\mathfrak{H}\to K^*$ satisfying

$$T(P)T(Q)=f(P,Q)T(PQ).$$

Then associativity of $T(P)$, $T(Q)$, $T(R)$ $(P, Q, R\in\mathfrak{H})$ yields the relations

$$f(PQ,R)f(P,Q)=f(P,QR)f(Q,R)$$

for all P, Q, R in $\mathfrak{H}$, i.e. f is a 2-cocycle of $\mathfrak{H}$ with values in K^* (under the trivial action of $\mathfrak{H}$ on K^*). This 2-cocycle f is called the *factor set* of ρ w.r.t. the section T.

Let T' be another section for ρ and f' be the factor set of ρ w.r.t. T'. Then there is a mapping $t:\mathfrak{H}\to K^*$ with $T'(H)=t(H)T(H)$ for any $H\in\mathfrak{H}$ and we have

$$f'(P,Q)=t(P)t(Q)t(PQ)^{-1}f(P,Q)$$

for all P, Q in $\mathfrak{H}$, i.e. f and f' are cohomologous. Thus the cohomology class c_ρ of f is independent on the choice of sections for ρ. We note that any cocycle in c_ρ is a factor set of ρ w.r.t. a certain section for ρ. $c_\rho\in \mathrm{H}^2(\mathfrak{H}, K^*)$ is called the cohomology class *associated to* the projective representation ρ. Also we shall say that ρ *belongs to* c_ρ. If $\rho_1\sim\rho_2$, we have $c_{\rho_1}=c_{\rho_2}$. A projective representation $\rho:\mathfrak{H}\to \mathrm{PGL}(V)$ has a section T which is a homomorphism $\mathfrak{H}\to \mathrm{GL}(V)$ if and only if $c_\rho=1$.

When K is the field of all complex numbers C, the group $\mathrm{H}^2(\mathfrak{H}, \mathrm{C}^*)$ is called the multiplier of $\mathfrak{H}$ and is denoted by $\mathfrak{M}(\mathfrak{H})$. Let $\mathfrak{H}$ be a finite group. Then it is proved by Schur [1] that $\mathfrak{M}(\mathfrak{H})$ is a finite abelian group and for any $c\in\mathfrak{M}(\mathfrak{H})$ $c^h=1$ where h is the order of $\mathfrak{H}$. We shall prove a slightly more general fact concerning this in § 3.1.

PROPOSITION 1.2. (Schur [1]) *Let $\mathfrak{H}$ be a finite group and K a field. Then, for any $c\in\mathrm{H}^2(\mathfrak{H}, K^*)$, there exists a projective representation ρ of $\mathfrak{H}$ in a finite dimensional vector space over K which belongs to c i.e. $c_\rho=c$.*

PROOF. Let f be a cocycle in c and V be a vector space with a base $\{e_H\}_{H\in\mathfrak{H}}$. We define a mapping $T:\mathfrak{H}\to \mathrm{GL}(V)$ by

$$T(P)\,e_Q=f(P,Q)\,e_{PQ}\qquad (P, Q\in\mathfrak{H}).$$

Then we have

$$\begin{aligned}T(P)T(Q)\,e_R&=T(P)f(Q,R)\,e_{QR}=f(P,QR)f(Q,R)\,e_{PQR}\\&=f(P,Q)f(PQ,R)\,e_{PQR}=f(P,Q)T(PQ)\,e_R\end{aligned}$$

for $P, Q, R\in\mathfrak{H}$, i.e. $T(P)T(Q)=f(P,Q)T(PQ)$. Hence T is a section of a projective representation ρ such that $c_\rho = c$. This completes the proof.

1.3. Central group extension and Hochschild-Serre's exact sequence.

Let $\mathfrak{H}$ be a group. A pair $(\mathfrak{G}, \pi)$ of a group $\mathfrak{G}$ and a surjective homomorphism $\pi: \mathfrak{G} \to \mathfrak{H}$ is called a group extension of $\mathfrak{H}$. $(\mathfrak{G}, \pi)$ is called central if the kernel $\mathfrak{A}$ of π is included in the center of $\mathfrak{G}$. Two group extensions $(\mathfrak{G}_i, \pi_i)$ $(i=1, 2)$ are called to be equivalent (in notation: $(\mathfrak{G}_1, \pi_1) \sim (\mathfrak{G}_2, \pi_2)$) if there exists an isomorphism $\sigma: \mathfrak{G}_1 \to \mathfrak{G}_2$ such that $\pi_2 \circ \sigma = \pi_1$.[6] When the kernel of a group extension is fixed, it is convenient to take more strong equivalence relation. Namely, let $(\mathfrak{G}_i, \pi_i)$ $(i=1, 2)$ be group extensions of $\mathfrak{H}$ by the kernel $\mathfrak{A}$. Then these are called to be strongly equivalent if there exists an isomorphism $\sigma: \mathfrak{G}_1 \to \mathfrak{G}_2$ such that $\pi_2 \circ \sigma = \pi_1$ and the restriction of σ to $\mathfrak{A}$ is the identity mapping.

A mapping $u: \mathfrak{H} \to \mathfrak{G}$ is called a section for $(\mathfrak{G}, \pi)$ if $\pi(u(H)) = H$ for any $H \in \mathfrak{H}$. Then we have

$$A(P, Q) = u(P)\, u(Q)\, u(PQ)^{-1} \in \mathfrak{A}$$

for any $P, Q \in \mathfrak{H}$. If $(\mathfrak{G}, \pi)$ is central, then the mapping $A: \mathfrak{H} \times \mathfrak{H} \to \mathfrak{A}$ defined by $(P, Q) \to A(P, Q)$ is an $\mathfrak{A}$-valued 2-cocycle of $\mathfrak{H}$ (under the trivial action of $\mathfrak{H}$ on $\mathfrak{A}$) i.e. $A \in \mathrm{Z}^2(\mathfrak{H}, \mathfrak{A})$. This cocycle is called the factor set of the extension $(\mathfrak{G}, \pi)$ w.r.t. the section u. Let u' be another section of $(\mathfrak{G}, \pi)$ and A' be the factor set w.r.t. u'. Then A and A' are cohomologous and the cohomology class C of A is independent on the choice of sections. This cohomology class $C \in \mathrm{H}^2(\mathfrak{H}, \mathfrak{A})$ is called the cohomology class associated to $(\mathfrak{G}, \pi)$ and denoted by $C((\mathfrak{G}, \pi))$. It is easily seen that $(\mathfrak{G}_i, \pi_i)$ $(i=1, 2)$ with the same kernel $\mathfrak{A}$ are strongly equivalent if and only if $C((\mathfrak{G}_1, \pi_1)) = C((\mathfrak{G}_2, \pi_2))$. The following is well known.

PROPOSITION 1.3. *Let $\mathfrak{H}$ be a group and $\mathfrak{A}$ an abelian group. Then, for any $C \in \mathrm{H}^2(\mathfrak{H}, \mathfrak{A})$, there exists a central group extension $(\mathfrak{G}, \pi)$ of $\mathfrak{H}$ such that the kernel of π is $\mathfrak{A}$ and $C((\mathfrak{G}, \pi)) = C$.*

Now let Ω be an abelian group on which $\mathfrak{H}, \mathfrak{A}, \mathfrak{G}$ act trivially. Then we have an exact sequence of cohomology groups (Hochschild-Serre [12]):

$$1 \to \mathrm{H}^1(\mathfrak{H}, \Omega) \xrightarrow{i_1} \mathrm{H}^1(\mathfrak{G}, \Omega) \xrightarrow{r_1} \mathrm{H}^1(\mathfrak{A}, \Omega) \xrightarrow{\tau} \mathrm{H}^2(\mathfrak{H}, \Omega) \xrightarrow{i_2} \mathrm{H}^2(\mathfrak{G}, \Omega) \tag{5}$$

where i_1, i_2 are the inflation mappings and r_1 is the restriction mapping. The mapping τ is called the transgression mapping[7] and is given as follows. Let u be any section of $(\mathfrak{G}, \pi)$ and A be the factor set of $(\mathfrak{G}, \pi)$ w.r.t. u. Let $\chi \in \mathrm{H}^1(\mathfrak{A}, \Omega)$.

6) Schur [2] introduced the equivalence relations of three kinds. This equivalence relation is of the first kind.

7) The mapping given in [12] is $\chi \to \tau(\chi)^{-1}$ $(\chi \in \mathrm{H}^1(\mathfrak{A}, \Omega))$.

Then the mapping $\chi\circ A:\mathfrak{H}\times\mathfrak{H}\to\Omega$ given by $(P,Q)\to\chi(A(P,Q))$ is a 2-cocycle in $Z^2(\mathfrak{H},\Omega)$ and the cohomology class c of $\chi\circ A$ is independent on the choice of the section. This cohomology class $c\in H^2(\mathfrak{H},\Omega)$ is the image of χ by the transgression mapping τ. It is easily seen that τ depends only on the cohomology class $C\in H^2(\mathfrak{H},\mathfrak{A})$ corresponding to $(\mathfrak{G},\pi)$. Hence we shall denote by τ_C the transgression mapping.

1.4. Linearization of a projective representation.

Let $(\mathfrak{G},\pi)$ be a central group extension of a finite group $\mathfrak{H}$ with the kernel $\mathfrak{A}$. Let V be a finite dimensional vector space over a field K and

$$\Gamma:\mathfrak{G}\to GL(V)$$

be a linear representation of $\mathfrak{G}$ such that $\Gamma(\mathfrak{A})\subset K^*1_V$. Then the restriction $\chi_\Gamma=\Gamma|\mathfrak{A}$ belongs to $\mathrm{Hom}(\mathfrak{A},K^*)=H^1(\mathfrak{A},K^*)$ if we identify K^*1_V with K^* naturally. Clearly if $\Gamma_1\sim\Gamma_2$, then $\chi_{\Gamma_1}=\chi_{\Gamma_2}$. Moreover Γ induces naturally a projective representation

$$\rho=\rho_\Gamma:\mathfrak{H}\to PGL(V).$$

More explicitly, taking any section u of $(\mathfrak{G},\pi)$, ρ is given by $\rho(H)=\Gamma(u(H))$ mod K^*1_V $(H\in\mathfrak{H})$, which is independent on the choice of the section u. Clearly if $\Gamma_1\sim\Gamma_2$, then $\rho_{\Gamma_1}\sim\rho_{\Gamma_2}$. We shall say that the projective representation $\rho=\rho_\Gamma$ of $\mathfrak{H}$ is *linearized by* the linear representation Γ of $\mathfrak{G}$.

Now fix a field K. Let $\mathfrak{R}(\mathfrak{G},\mathfrak{A})$ be the set of all equivalent classes of finite dimensional linear representations of $\mathfrak{G}$ over K such that the image of $\mathfrak{A}$ by the representation consists of scalar multiples of the identity transformation of the representation space. Let $\mathfrak{P}(\mathfrak{H})$ be the set of all equivalent classes of finite dimensional projective representations of $\mathfrak{H}$ over K. Then we have, as stated above, the mappings

$$\pi:\mathfrak{R}(\mathfrak{G},\mathfrak{A})\to\mathfrak{P}(\mathfrak{H})$$
$$\Psi_1:\mathfrak{R}(\mathfrak{G},\mathfrak{A})\to H^1(\mathfrak{A},K^*)$$

which are defined by $\Gamma\to\rho_\Gamma$ and $\Gamma\to\chi_\Gamma$ respectively. Also we have, as stated in § 1.2, the mapping

$$\Psi_2:\mathfrak{P}(\mathfrak{H})\to H^2(\mathfrak{H},K^*)$$

defined by $\rho\to c_\rho$. Furthermore we have, as stated in § 1.3, the mapping

$$\tau:H^1(\mathfrak{A},K^*)\to H^2(\mathfrak{H},K^*).$$

Thus we obtain the following fundamental diagram of mappings.

$$\begin{tikzcd} \mathfrak{R}(\mathfrak{G}, \mathfrak{A}) \arrow[r, "\Pi"] \arrow[d, "\Psi_1"'] & \mathfrak{P}(\mathfrak{H}) \arrow[d, "\Psi_2"] \\ \mathrm{H}^1(\mathfrak{A}, K^*) \arrow[r, "\tau"'] & \mathrm{H}^2(\mathfrak{H}, K^*) \end{tikzcd} \tag{6}$$

Then we have

PROPOSITION 1.4. 1) *The diagram* (6) *is commutative i.e.* $\Psi_2 \circ \Pi = \tau \circ \Psi_1$.

2) *Let* $\chi \in \mathrm{H}^1(\mathfrak{A}, K^*)$ *and* $\tilde{\rho} \in \mathfrak{P}(\mathfrak{H})$ *such that* $\tau(\chi) = \Psi_2(\tilde{\rho})$. *Then there exists a* $\tilde{\Gamma} \in \mathfrak{R}(\mathfrak{G}, \mathfrak{A})$ *such that* $\Pi(\tilde{\Gamma}) = \tilde{\rho}$ *and* $\Psi_1(\tilde{\Gamma}) = \chi$ (*i.e.* $\rho_\Gamma = \rho$[8] *and* $\chi_\Gamma = \chi$).

3) Ψ_1 *and* Ψ_2 *are surjective.*

4) Π *is surjective if and only if* τ *is surjective.*

PROOF. 1) Straightforward.

2) Let u be a section of $(\mathfrak{G}, \pi)$ with $u(I)=I$ and T be a section of (ρ, V). Let A be the factor set of u and f be the factor set of T. Since $\chi \circ A$ and f are cohomologous, replacing T if necessary by a suitable section of ρ, we may assume $\chi \circ A = f$. Now $u(I)=I$ implies $A(I, H)=A(H, I)=I$ and $f(I, H)=f(H, I)=1$ i.e. A and f are normalized. Hence $T_I = 1_V$. We define the mapping $\Gamma: \mathfrak{G} \to \mathrm{GL}(V)$ by $\Gamma(A\,u(H)) = \chi(A)\,T(H)$ $(A \in \mathfrak{A}, H \in \mathfrak{H})$. Then it is easily seen that Γ is a linear representation of $\mathfrak{G}$ in V, $\rho_\Gamma = \rho$ and $\chi_\Gamma = \chi$.

3), 4) are immediate consequences of 1), 2) and Proposition 1.2. q.e.d.

The image of Π means the classes of projective representations of $\mathfrak{H}$ which can be linearized by $(\mathfrak{G}, \pi)$. Hence it is important to construct a central group extension $(\mathfrak{G}, \pi)$ such that Π is surjective, or equivalently, τ is surjective. When $K=\mathbf{C}$ (complex numbers) and $\mathfrak{H}$ is a finite group, it is proved by Schur [1] that there exists a central group extension $(\mathfrak{G}, \pi)$ of $\mathfrak{H}$ such that τ is bijective; such a group $\mathfrak{G}$ is called a representation-group of $\mathfrak{H}$ (over a field K). In Schur's case, $\mathfrak{G}$ is a finite group whose order is equal to $[\mathfrak{H}:I][\mathfrak{M}(\mathfrak{H}):1]$. However, when K is an algebraic number field, $\mathfrak{M}(\mathfrak{H}) = \mathrm{H}^2(\mathfrak{H}, K^*)$ is not necessarily finite even if $\mathfrak{H}$ is finite. In such a case there is no finite representation-group.

§ 2. 2-cohomology and pairings.

2.1. An operator on cocycles.

Let $\mathfrak{H}$ be a group which acts on an abelian group Ω. We take an element P of $\mathfrak{H}$ and any subgroup $\mathfrak{Z}$ of $\mathfrak{H}$. For any $f \in \mathrm{C}^n(\mathfrak{H}, \Omega)$, we denote by f_P the $(n-1)$-cochain in $\mathrm{C}^{n-1}(\mathfrak{Z}, \Omega)$ defined by the formula

$$f_P(X_1, \cdots, X_{n-1}) = \prod_{i=0}^{n-1} f(X_1, \cdots, X_i, P, X_{i+1}, \cdots, X_{n-1})^{(-1)^i}$$

8) ρ is a representative of an equivalence class $\tilde{\rho}$ in $\mathfrak{P}(\mathfrak{H})$. Similarly Γ is also a representative.

where $P_0=P$, $P_i=(X_1\cdots X_i)^{-1}P(X_1\cdots X_i)$ $(1\leqq i\leqq n-1)$.

For $n=1$, we have

$$f_P(\ )=f(P).$$

For $n=2$, we have

$$f_P(X)=f(P,X)f(X,X^{-1}PX)^{-1}. \qquad (X\in\mathfrak{Z}) \tag{7}$$

Then we have the followings respectively in the above cases.

$$\begin{aligned}(\delta f)_P(X)&=(\delta f)(P,X)(\delta f)(X,P_1)^{-1}\\&={}^Pf(X)f(PX)^{-1}f(P)^Xf(P_1)^{-1}f(XP_1)f(X)^{-1}\\&={}^Xf_{X^{-1}PX}(\ )^{-1}f_P(\ )^Pf(X)f(X)^{-1}\end{aligned}$$

$$\begin{aligned}(\delta f)_P(X,Y)&=(\delta f)(P,X,Y)(\delta f)(X,P_1,Y)^{-1}(\delta f)(X,Y,P_2)\\&={}^Pf(X,Y)f(PX,Y)^{-1}f(P,XY)f(P,X)^{-1}\\&\quad{}^Xf(P_1,Y)^{-1}f(XP_1,Y)f(X,P_1Y)^{-1}f(X,P_1)\\&\quad{}^Xf(Y,P_2)f(XY,P_2)^{-1}f(X,YP_2)f(X,Y)^{-1}\\&={}^X\{f(P_1,Y)f(Y,P_2)^{-1}\}^{-1}\{f(P,XY)f(XY,P_2)^{-1}\}\\&\quad\{f(P,X)f(X,P_1)^{-1}\}^{-1}\,{}^Pf(X,Y)f(X,Y)^{-1}\\&={}^Xf_{X^{-1}PX}(Y)^{-1}f_P(XY)f_P(X)^{-1}\,{}^Pf(X,Y)f(X,Y)^{-1}\end{aligned}$$

If f is a cocycle and the action of P is trivial, then we have

$$f_P(XY)={}^Xf_{X^{-1}PX}(Y)f_P(X) \tag{8}$$

In the following, we assume that the action of P is trivial and $\mathfrak{Z}$ is included in the centralizer of P in $\mathfrak{H}$. Then we have

$$(\delta f)_P\,\delta f_P=1 \tag{9}$$

for any $f\in C^n(\mathfrak{H},\Omega)$. This formula follows from the above computations for $n=1,2$.[9] Hence the mapping $f\to f_P$ induces a homomorphism

$$H^n(\mathfrak{H},\Omega)\to H^{n-1}(\mathfrak{Z},\Omega) \qquad (n\geqq 1);$$

we denote by c_P the image of $c\in H^n(\mathfrak{H},\Omega)$ under this mapping.

2.2. 2-cohomology of the direct product of groups.

In the following we assume that any group considered acts on an abelian group Ω trivially. Let $\mathfrak{H}_1$ and $\mathfrak{H}_2$ be subgroups of a group $\mathfrak{H}$ such that $[\mathfrak{H}_1,\mathfrak{H}_2]=\{I\}$ i.e. $H_1H_2=H_2H_1$ for all $H_i\in\mathfrak{H}_i$ $(i=1,2)$.

For any cocycle $f\in Z^2(\mathfrak{H},\Omega)$, we consider the mapping $\varphi:\mathfrak{H}_1\times\mathfrak{H}_2\to\Omega$ defined by the formula

9) We omit the proof of the formula (9) for $n\geqq 3$, since we shall not use it for $n\geqq 3$.

$$\varphi(H_1, H_2)=f(H_1, H_2)\, f(H_2, H_1)^{-1} \qquad (H_i \in \mathfrak{H}_i). \tag{10}$$

Then φ is a pairing of $\mathfrak{H}_1$ and $\mathfrak{H}_2$ into Ω.[10] In fact, we have $\varphi(H_1, H_2)=f_{H_1}(H_2)$ $=f_{H_2}(H_1)^{-1}$. However, for any $H_i \in \mathfrak{H}_i$, $\mathfrak{H}_j$ $(j \neq i)$ is included in the centralizer of H_i in $\mathfrak{H}$ and f_{H_i} is in $\mathrm{Z}^1(\mathfrak{H}_j, \Omega)=\mathrm{Hom}(\mathfrak{H}_j, \Omega)$. Moreover we see by (9) that φ depends only on the cohomology class of f. Thus we obtain a homomorphism

$$\mathrm{H}^2(\mathfrak{H}, \Omega) \to \mathrm{P}(\mathfrak{H}_1, \mathfrak{H}_2\,;\, \Omega) \tag{11}$$

where $\mathrm{P}(\mathfrak{H}_1, \mathfrak{H}_2\,;\, \Omega)$ is the group of all pairings of $\mathfrak{H}_1$ and $\mathfrak{H}_2$ into Ω. Then we have the following theorem.

THEOREM 2.1. *Let a group $\mathfrak{H}$ be decomposed into the direct product of two normal subgroups $\mathfrak{H}_1$ and $\mathfrak{H}_2$. We denote by c_i the restriction of $c \in \mathrm{H}^2(\mathfrak{H}, \Omega)$ to $\mathfrak{H}_i$ $(i=1, 2)$ and by φ_c the pairing which corresponds to c by* (11). *Then, by the mapping $c \to (c_1, c_2, \varphi_c)$, we have the following isomorphism.*

$$\mathrm{H}^2(\mathfrak{H}, \Omega) \cong \mathrm{H}^2(\mathfrak{H}_1, \Omega) \times \mathrm{H}^2(\mathfrak{H}_2, \Omega) \times \mathrm{P}(\mathfrak{H}_1, \mathfrak{H}_2\,;\, \Omega)$$

PROOF. Let f_i be any normalized cocycle of $\mathfrak{H}_i$ $(i=1, 2)$ and φ in $\mathrm{P}(\mathfrak{H}_1, \mathfrak{H}_2\,;\, \Omega)$. We define a 2-cochain f of $\mathfrak{H}$ by the formula

$$f(P_1P_2, Q_1Q_2)=f_1(P_1, Q_1)\, f_2(P_2, Q_2)\varphi(P_1, Q_2)$$

for $P_i, Q_i \in \mathfrak{H}_i$ $(i=1, 2)$. Then it follows easily that f is a 2-cocycle of $\mathfrak{H}$. Moreover its restriction to $\mathfrak{H}_i$ is f_i $(i=1, 2)$ and the corresponding pairing is φ. This proves that the homomorphism $c \to (c_1, c_2, \varphi_c)$ is surjective.

Let f be a 2-cocycle of $\mathfrak{H}$ such that its restriction f_i to $\mathfrak{H}_i$ is a coboundary of $\mathfrak{H}_i$ $(i=1, 2)$ and the corresponding pairing is trivial; we write $f_i=\delta g_i$ where g_i is a 1-cochain of $\mathfrak{H}_i$ $(i=1, 2)$. If we define a 1-cochain g of $\mathfrak{H}$ by the formula $g(P_1P_2)=g_1(P_1)g_2(P_2)$, then the restrictions of $f(\delta g)^{-1}$ to the $\mathfrak{H}_i$ are trivial. Hence we can assume that the f_i are trivial i.e.

$$f(P_1, Q_1)=f(P_2, Q_2)=1$$

for $P_i, Q_i \in \mathfrak{H}_i$ $(i=1, 2)$.

Then we have

$$1=(\delta f)(P_1P_2, Q_1, Q_2)^{-1}=f(Q_1, Q_2)^{-1}f(P_1P_2Q_1, Q_2)f(P_1P_2, Q_1Q_2)^{-1}f(P_1P_2, Q_1)\,,$$
$$1=(\delta f)(P_1Q_1, P_2, Q_2)=f(P_2, Q_2)f(P_1Q_1P_2, Q_2)^{-1}f(P_1Q_1, P_2Q_2)f(P_1Q_1, P_2)^{-1}\,,$$
$$1=(\delta f)(P_2, P_1, Q_1)=f(P_1, Q_1)f(P_2P_1, Q_1)^{-1}f(P_2, P_1Q_1)f(P_2, P_1)^{-1}\,.$$

Also we have

10) This means $\varphi(P_1Q_1, H_2)=\varphi(P_1, H_2)\varphi(Q_1, H_2)$ and $\varphi(H_1, P_2Q_2)=\varphi(H_1, P_2)\varphi(H_1, Q_2)$ $(P_i, Q_i, H_i \in \mathfrak{H}_i)$.

$$1=\varphi(P_1Q_1, P_2)=f(P_1Q_1, P_2)f(P_2, P_1Q_1)^{-1},$$
$$1=\varphi(P_1, P_2)^{-1}=f(P_1, P_2)^{-1}f(P_2, P_1).$$

From the above five equalities, it follows easily that

$$1=f(P_1P_2, Q_1Q_2)^{-1}f(Q_1, Q_2)^{-1}f(P_1Q_1, P_2Q_2)f(P_1, P_2)^{-1}.$$

Therefore we have $f=\partial l$ when we define a 1-cochain l of $\mathfrak{H}$ by the formula $l(P_1P_2)=f(P_1, P_2)^{-1}$. This proves that the homomorphism $c\to(c_1, c_2, \varphi_c)$ is injective. q.e.d.

Theorem 2.1 is easily generalized as follows. Let $\mathfrak{H}$ be a group which is decomposed into the direct product of normal subgroups $\mathfrak{H}_1, \mathfrak{H}_2, \cdots, \mathfrak{H}_m$. Then we have an isomorphism

$$\mathrm{H}^2(\mathfrak{H}, \Omega)\cong\prod_{i=1}^{m}\mathrm{H}^2(\mathfrak{H}, \Omega)\times\prod_{1\leqq j<k\leqq m}\mathrm{P}(\mathfrak{H}_j, \mathfrak{H}_k; \Omega).$$

This can be proved by induction on m, since we have naturally

$$\mathrm{P}(\mathfrak{H}_1\times\cdots\times\mathfrak{H}_m, \mathfrak{H}_{m+1}; \Omega)\cong\prod_{j=1}^{m}\mathrm{P}(\mathfrak{H}_j, \mathfrak{H}_{m+1}; \Omega).$$

Let us apply this to the case where each $\mathfrak{H}_i$ is cyclic.

COROLLARY. *Let $\mathfrak{H}$ be a finite abelian group which is decomposed into the direct product of m cyclic subgroups $\mathfrak{H}_i$ of order ε_i $(1\leqq i\leqq m)$. Then we have*

$$\mathrm{H}^2(\mathfrak{H}, \Omega)\cong\prod_{i=1}^{m}\Omega/\Omega^{\varepsilon_i}\times\prod_{1\leqq j<k\leqq m}\Omega_{(d_{jk})}$$

where $d_{jk}=(\varepsilon_j, \varepsilon_k)$.[11]

PROOF. Clearly we have $\mathrm{P}(\mathfrak{H}_j, \mathfrak{H}_k; \Omega)\cong\Omega_{(d_{jk})}$. Moreover it is well known that $\mathrm{H}^2(\mathfrak{H}_i, \Omega)\cong\Omega/\Omega^{\varepsilon_i}$, since $\mathfrak{H}_i$ is cyclic of order ε_i. The corollary is thereby proved.

We shall give in Theorem 2.2 another description of $\mathrm{H}^2(\mathfrak{H}, \Omega)$.

2.3. Abelian cocycles and anti-symmetric pairings.

Let $\mathfrak{H}$ be a group and Ω an abelian group fixed once for all. We shall call a pairing of $\mathfrak{H}$ and $\mathfrak{H}$ itself into Ω simply a pairing of $\mathfrak{H}$ into Ω. We consider the following condition on a pairing φ of $\mathfrak{H}$ into Ω.

(12) $$\varphi(H, H)=1 \qquad \text{for all } H\in\mathfrak{H}.$$

This implies $\varphi(P, Q)=\varphi(Q, P)^{-1}$ for all $P, Q\in\mathfrak{H}$. In fact,

$$1=\varphi(PQ, PQ)=\varphi(P, PQ)\varphi(Q, PQ)$$
$$=\varphi(P, P)\varphi(P, Q)\varphi(Q, P)\varphi(Q, Q)=\varphi(P, Q)\varphi(Q, P).$$

We call a pairing of $\mathfrak{H}$ into Ω satisfying (12) *anti-symmetric*; we denote by

11) See the notation in §1.1. $(\varepsilon_j, \varepsilon_k)$ means the greatest common divisor of ε_j and ε_k.

$P_{a.s.}(\mathfrak{H}, \Omega)$ the group of all anti-symmetric pairings of $\mathfrak{H}$ into Ω.

In the following we shall consider abelian groups exclusively. Let $\mathfrak{H}$ be an abelian group. We consider the following condition on a 2-cocycle f of $\mathfrak{H}$ in Ω.

$$f(P, Q)=f(Q, P) \qquad \text{for all } P, Q\in\mathfrak{H}. \tag{13}$$

We call a 2-cocycle of $\mathfrak{H}$ in Ω satisfying (13) *abelian*; we denote by $H^2_{abel}(\mathfrak{H}, \Omega)$ the subgroup of $H^2(\mathfrak{H}, \Omega)$ consisting of cohomology classes which contain abelian cocycles. We note that any cocycle which is cohomologous to an abelian cocycle is also abelian; we call $c\in H^2_{abel}(\mathfrak{H}, \Omega)$ an abelian cohomology class.[12]

We have clearly

$$H^2_{abel}(\mathfrak{H}, \Omega)=H^2(\mathfrak{H}, \Omega) \qquad \text{for any cyclic group } \mathfrak{H}.$$

Moreover by the isomorphism in Theorem 2.1 we have

$$H^2_{abel}(\mathfrak{H}, \Omega)\cong H^2_{abel}(\mathfrak{H}_1, \Omega)\times H^2_{abel}(\mathfrak{H}_2, \Omega) \tag{14}$$

if $\mathfrak{H}$ is decomposed into the direct product of abelian subgroups $\mathfrak{H}_i$ $(i=1, 2)$.

Therefore we have

PROPOSITION 2.1. *Let a group $\mathfrak{H}$ be decomposed into the direct product of m cyclic subgroups of order ε_i $(1\leq i\leq m)$. Then we have*

$$H^2_{abel}(\mathfrak{H}, \Omega)\cong \prod_{i=1}^{m} \Omega/\Omega^{\varepsilon_i}.$$

Moreover, if Ω is also decomposed into the direct product of n cyclic subgroups of order η_j $(1\leq j\leq n)$, then we have

$$H^2_{abel}(\mathfrak{H}, \Omega)\cong \prod_{i=1}^{m} \prod_{j=1}^{n} Z_{(\varepsilon_i, \eta_j)}$$

where $Z_{(\varepsilon_i, \eta_j)}$ denotes the cyclic group of order (ε_i, η_j).

PROOF. The first part is clear by the above consideration. We easily see that

$$(\prod_j Z_{\eta_j})/(\prod_j Z_{\eta_j})^{\varepsilon_i}\cong \prod_j (Z_{\eta_j}/Z_{\eta_j}^{\varepsilon_i})\cong \prod_j Z_{(\varepsilon_i, \eta_j)}.$$

This completes the proof.

Now let $\mathfrak{H}$ be an abelian group. Then we have the homomorphism, as defined in § 2.2,

$$H^2(\mathfrak{H}, \Omega)\rightarrow P(\mathfrak{H}, \mathfrak{H}; \Omega)$$

by setting $\mathfrak{H}_1=\mathfrak{H}_2=\mathfrak{H}$ in (11). The image of this homomorphism is included in $P_{a.s.}(\mathfrak{H}, \Omega)$ because of (10). Thus we obtain the fundamental homomorphism

12) This is equivalent to the condition that the group extension of $\mathfrak{H}$ by Ω corresponding to c is abelian.

$$\mathrm{H}^2(\mathfrak{H}, \Omega) \to \mathrm{P}_{\mathrm{a.s.}}(\mathfrak{H}, \Omega) \qquad \text{for an abelian group } \mathfrak{H}.$$

It is easily seen that $\mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H}, \Omega)$ is the kernel of this homomorphism. In detail, we have the following.

THEOREM 2.2. *Let $\mathfrak{H}$ be a finitely generated abelian group and Ω an arbitrary abelian group. Then we have the splitting exact sequence*

$$1 \to \mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H}, \Omega) \to \mathrm{H}^2(\mathfrak{H}, \Omega) \to \mathrm{P}_{\mathrm{a.s.}}(\mathfrak{H}, \Omega) \to 1$$

defined by the natural homomorphisms.

PROOF. Let φ be any anti-symmetric pairing of $\mathfrak{H}$ into Ω. Let $\mathfrak{H}$ be the direct product of m cyclic subgroups generated by S_i $(1 \leqq i \leqq m)$ and we define a pairing f of $\mathfrak{H}$ into Ω by the formula

$$f(S_i, S_j) = \begin{cases} 1 & \text{if } i \leqq j, \\ \varphi(S_i, S_j) & \text{if } i > j. \end{cases}$$

We note that any pairing f of a group $\mathfrak{H}$ into Ω is always a 2-cocycle of $\mathfrak{H}$ in Ω. In fact,

$$\begin{aligned}(\partial f)(P, Q, R) &= f(Q, R) f(PQ, R)^{-1} f(P, QR) f(P, Q)^{-1} \\ &= f(Q, R) f(P, R)^{-1} f(Q, R)^{-1} f(P, Q) f(P, R) f(P, Q)^{-1} \\ &= 1 .\end{aligned}$$

Hence we have a 2-cocycle f of $\mathfrak{H}$ in Ω and easily see that φ corresponds to f, which proves that the homomorphism $\mathrm{H}^2(\mathfrak{H}, \Omega) \to \mathrm{P}_{\mathrm{a.s.}}(\mathfrak{H}, \Omega)$ is surjective.

The splitting of the exact sequence follows by induction on m since the isomorphism in Theorem 2.1 induces the isomorphism (14). q.e.d.

As mentioned in the proof of Theorem 2.2, any pairing is a 2-cocycle; we call such a 2-cocycle a *pairing cocycle* and denote by $\mathrm{H}^2_{\mathrm{pair}}(\mathfrak{H}, \Omega)$ the subgroup of $\mathrm{H}^2(\mathfrak{H}, \Omega)$ consisting of cohomology classes which contain pairing cocycles. Then we have, from the proof of Theorem 2.2, the following.

COROLLARY 1. *Let $\mathfrak{H}$ be a finitely generated abelian group and Ω an arbitrary abelian group. Then $\mathrm{H}^2(\mathfrak{H}, \Omega)$ is generated by two subgroups $\mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H}, \Omega)$ and $\mathrm{H}^2_{\mathrm{pair}}(\mathfrak{H}, \Omega)$.*

REMARK. If $\mathfrak{H}$ contains no element of even order, then $\mathrm{H}^2(\mathfrak{H}, \Omega)$ is decomposed into the direct product of $\mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H}, \Omega)$ and $\mathrm{H}^2_{\mathrm{pair}}(\mathfrak{H}, \Omega)$. In fact, by (14), we may assume that $\mathfrak{H}$ is a cyclic group of odd order h. Let S be a generator of $\mathfrak{H}$ and f a pairing cocycle. If we set $f(S, S) = \omega$, we have $\omega^h = 1$. Since $h(h-1)/2$ is divisible by h,

$$\omega^{1+2+\cdots+(i-1)} \qquad (i \geqq 1)$$

depends only on i modulo h; we denote by $g(S^i)$ this value. Thus we obtain a

1-cochain g of $\mathfrak{H}$ in Ω and easily see that $f=(\delta g)^{-1}$, which implies $\mathrm{H}^2_{\mathrm{pair}}(\mathfrak{H},\Omega)=\{1\}$. This completes the proof of the direct product decomposition.

COROLLARY 2. *Let $\mathfrak{H}$ be a finitely generated abelian group and Ω an infinitely divisible*[13] *abelian group. Then we have*

$$\mathrm{H}^2_{\mathrm{pair}}(\mathfrak{H},\Omega)=\mathrm{H}^2(\mathfrak{H},\Omega)\cong \mathrm{P}_{\mathrm{a.s.}}(\mathfrak{H},\Omega)$$

by the natural mapping.

PROOF. By the assumption and Proposition 2.1, we have $\mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H},\Omega)=\{1\}$. Therefore the Corollary follows from Theorem 2.2 and Corollary 1.

§ 3. Central group extensions of a finite group.

3.1. The multiplier.

In § 3, we shall consider a suitably large field K. For any positive integer d, a field K is called d-divisible, if the multiplicative group K^* is d-divisible (Cf. § 1.1.). We have the following proposition which will be used later only in the case that $n=2$ and the action is trivial.

PROPOSITION 3.1. *Let K be a field and $\mathfrak{H}$ be a finite group of order h acting on K^* such that K is h-divisible i.e. the mapping $\lambda\to\lambda^h$ $(\lambda\in K)$ is surjective.*[14] *Then, for any positive integer n, the followings hold.*

1) $c^h=1$ *for any* $c\in \mathrm{H}^n(\mathfrak{H},K^*)$.

2) $\mathrm{H}^n(\mathfrak{H},K^*)$ *is a finite abelian group whose order is not divisible by the characteristic of K.*

3) *The following exact sequence splits.*

$$1\to \mathrm{B}^n(\mathfrak{H},K^*)\to \mathrm{Z}^n(\mathfrak{H},K^*)\to \mathrm{H}^n(\mathfrak{H},K^*)\to 1\,.$$

PROOF. 1) This follows from Proposition 1.1.1).

2) From 1), it follows that any $c\in \mathrm{H}^n(\mathfrak{H},K^*)$ has a finite order d dividing h and K is d-divisible. Hence, by Proposition 1.1.2), c contains a cocycle f of the same order d. Since the values of this cocycle f have the orders not divisible by the characteristic of K, d is not divisible by the characteristic of K. However there are only a finite number of those cocycles, since the values are h-th root of 1. Thus $\mathrm{H}^n(\mathfrak{H},K^*)$ is finite and its order is not divisible by the characteristic of K. This completes the proof of 2).

3) Let $c_1,\cdots,c_s$ be a base of the finite abelian group $\mathrm{H}^n(\mathfrak{H},K^*)$. We can take a cocycle $f_i\in c_i$ which has the same order as c_i for each i. Then $\mathrm{Z}^n(\mathfrak{H},K^*)$

13) This means that $\Omega^n=\Omega$ for any positive integer n. For example we can take $\Omega=K^*$ where K is an algebraically closed field.

14) This condition is valid for any algebraically closed field K.

is decomposed into the direct product of $B^n(\mathfrak{H}, K^*)$ and the subgroup generated by $f_1, \cdots, f_s$. This completes the proof of 3). q.e.d.

REMARK. Suppose that the action of a finite group $\mathfrak{H}$ is trivial. Let K be any field and $\bar{K}$ be the algebraic closure of K. Then $H^2(\mathfrak{H}, \bar{K}^*)$ is a finite abelian group by Proposition 3.1. We have the exact sequence (§ 1.1 (3))

$$H^1(\mathfrak{H}, \bar{K}^*) \to H^1(\mathfrak{H}, \bar{K}^*/K^*) \to H^2(\mathfrak{H}, K^*) \to H^2(\mathfrak{H}, \bar{K}^*) .$$

Clearly $H^1(\mathfrak{H}, \bar{K}^*)$ is finite. Hence it follows that $H^2(\mathfrak{H}, K^*)$ is finite if and only if $H^1(\mathfrak{H}, \bar{K}^*/K^*) = \mathrm{Hom}(\mathfrak{H}, \bar{K}^*/K^*)$ is finite. In particular, if $\mathfrak{H}$ coincides with its commutator subgroup $\mathfrak{H}'$, $H^2(\mathfrak{H}, K^*)$ is always finite for any field K. (Cf. [7]). But if not, $H^2(\mathfrak{H}, K^*)$ is not necessarily finite. For example, let K be any algebraic number field of finite degree. Then, $H^2(\mathfrak{H}, K^*)$ is infinite if $\mathfrak{H} \neq \mathfrak{H}'$.

Under the trivial action on coefficient groups, we have the following proposition (Cf. [9]) which will not be used later.

PROPOSITION 3.2. *Let K be an algebraically closed field of characteristic $p \geq 0$ and $\mathfrak{H}$ be a finite group of order h. Let Ω be an h-divisible subgroup of K^* containing all h-th roots of 1. Then for any $n>0$ the structure of $H^n(\mathfrak{H}, \Omega)$ depends only on $\mathfrak{H}$ and p; we denote by $\mathfrak{M}_p^n(\mathfrak{H})$ this group. Moreover we have*[15]

$$\mathfrak{M}_p^n(\mathfrak{H}) \cong \mathfrak{M}_0^n(\mathfrak{H})/\mathfrak{P} \qquad (p>0)$$

where $\mathfrak{P}$ is the p-Sylow subgroup of $\mathfrak{M}_0^n(\mathfrak{H})$.

PROOF. For the former part, it is sufficient[16] to prove that the natural homomorphism $H^n(\mathfrak{H}, \Omega) \to H^n(\mathfrak{H}, K^*)$ is bijective. The exact sequence $1 \to \Omega \to K^* \to K^*/\Omega \to 1$ yields the following exact sequence by (3).

$$H^{n-1}(\mathfrak{H}, K^*) \to H^{n-1}(\mathfrak{H}, K^*/\Omega) \to H^n(\mathfrak{H}, \Omega) \to H^n(\mathfrak{H}, K^*) \to H^n(\mathfrak{H}, K^*/\Omega)$$

It is easily seen that $(K^*/\Omega)_{(h)} = \{1\}$ by the assumption. Therefore we have $H^n(\mathfrak{H}, K^*/\Omega) = \{1\}$ for $n \geq 1$, by Proposition 1.1. Thus we have

$$1 \to H^n(\mathfrak{H}, \Omega) \to H^n(\mathfrak{H}, K^*) \to 1 \qquad \text{for } n \geqq 2.$$

For $n=1$, we have clearly the surjective homomorphism $H^0(\mathfrak{H}, K^*) \to H^0(\mathfrak{H}, K^*/\Omega)$ which implies that $H^1(\mathfrak{H}, \Omega) \to H^1(\mathfrak{H}, K^*)$ is injective. This completes the proof of the former part.

By the former part of Proposition, we have

$$\mathfrak{M}_0^n(\mathfrak{H}) \cong H^n(\mathfrak{H}, W),$$
$$\mathfrak{M}_p^n(\mathfrak{H}) \cong H^n(\mathfrak{H}, W/W_{(p)}) \qquad (p>0)$$

where W is the group of all roots of 1 in the complex number field and $W_{(p)}$ is

15) Of course $\mathfrak{M}_0^2(\mathfrak{H})$ is the multiplier of $\mathfrak{H}$ in Schur's sense.

16) Consider the algebraic closure of the prime field of characteristic p.

the subgroup of W consisting of p^ν-th roots ($\nu=0,1,2,\cdots$). The splitting exact sequence $1\to W_{(p)}\to W\to W/W_{(p)}\to 1$ yields the splitting exact sequence

$$1\to \mathrm{H}^n(\mathfrak{H}, W_{(p)})\to \mathrm{H}^n(\mathfrak{H}, W)\to \mathrm{H}^n(\mathfrak{H}, W/W_{(p)})\to 1.$$

$\mathrm{H}^n(\mathfrak{H}, W_{(p)})$ is a p-group and the order of $\mathrm{H}^n(\mathfrak{H}, W/W_{(p)})$ is not divisible by p. This completes the proof of the latter part.

3.2. Some types of central group extensions.

Let $\mathfrak{H}$ be a finite group of order h and $(\mathfrak{G},\pi)$ a central group extension of $\mathfrak{H}$ by the kernel $\mathfrak{A}$. As stated in §1.4, linearizations of projective representations of $\mathfrak{H}$ over a field K by $(\mathfrak{G},\pi)$ are closely related to the transgression mapping

$$\tau_{C(\mathfrak{G},\pi)}: \mathrm{H}^1(\mathfrak{A}, K^*)\to \mathrm{H}^2(\mathfrak{H}, K^*).$$

We shall define some types of central group extensions $(\mathfrak{G},\pi)$ according to the properties of $\tau_{C(\mathfrak{G},\pi)}$.

For the sake of simplicity, we fix a finite abelian group $\mathfrak{A}$ and assume that K satisfies the following two conditions. (Cf. Proposition 3.2.)

1) *K is h-divisible.* This means that the mapping of K into itself defined by $\lambda\to\lambda^h$ is surjective.

2) *K is $\mathfrak{A}$-cyclic.* This means that if $\mathfrak{A}$ has an element of order d, K contains a primitive d-th root of 1, whence $\mathfrak{A}\cong\mathrm{Hom}(\mathfrak{A}, K^*)$.

In the following, we fix such a field K. Moreover we denote by $\hat{\mathfrak{A}}$ the group $\mathrm{Hom}(\mathfrak{A}, K^*)=\mathrm{H}^1(\mathfrak{A}, K^*)$ and by $\mathfrak{M}(\mathfrak{H})$ the group $\mathrm{H}^2(\mathfrak{H}, K^*)$.

Let $(\mathfrak{G},\pi)$ be a central group extension of $\mathfrak{H}$ by $\mathfrak{A}$ and C be the cohomology class in $\mathrm{H}^2(\mathfrak{H},\mathfrak{A})$ associated to $(\mathfrak{G},\pi)$. We call $(\mathfrak{G},\pi)$ to be of *bijective type*, *surjective type*, *injective type* respectively if the associated transgression mapping τ_C is bijective, surjective, injective. A central group extension of bijective type is nothing but a representation-group (§1.4.). Furthermore we call $(\mathfrak{G},\pi)$ to be of *0-type* (or abelian type) if τ_C is trivial i.e. the image of τ_C consists of only the unit element. We may generalize the concept of 0-type as follows. Let δ_s be the natural homomorphism

$$\mathfrak{M}(\mathfrak{H})\to\mathfrak{M}(\mathfrak{H}^{(s)})\qquad (s=1,2,\cdots)$$

where $\mathfrak{H}^{(s)}$ is the s-th commutator subgroup of $\mathfrak{H}$. Then we call $(\mathfrak{G},\pi)$ to be of *s-type* if $\delta_s\circ\tau_C$ is trivial.

Now we have the following lemma by the assumptions on K.

LEMMA 3.1. *The following sequence defined by the natural homomorphisms is exact.*

$$1 \to \mathrm{Hom}(\mathfrak{H}, K^*) \to \mathrm{Hom}(\mathfrak{G}, K^*) \to \mathrm{Hom}(\mathfrak{A}, K^*) \to \mathrm{Hom}(\mathfrak{G}' \cap \mathfrak{A}, K^*) \to 1 .$$[17]

This exact sequence and the Hochschild-Serre's exact sequence (§ 1.3.) imply the following.

PROPOSITION 3.3. *Let* $(\mathfrak{G}, \pi)$ *be a central group extension of* $\mathfrak{H}$ *by* $\mathfrak{A}$. *Then*

1) $(\mathfrak{G}, \pi)$ *is of s-type if and only if* $\mathfrak{G}^{(s+1)} \cap \mathfrak{A} = \{I\}$.

2) $(\mathfrak{G}, \pi)$ *is of injective type if and only if* $\mathfrak{G}' \supset \mathfrak{A}$.

PROOF. π induces an isomorphism

$$\mathfrak{A}\mathfrak{G}^{(s)}/\mathfrak{A} \cong \mathfrak{H}^{(s)} .$$

Hence we have a central group extension $(\mathfrak{A}\mathfrak{G}^{(s)}, \pi|\mathfrak{A}\mathfrak{G}^{(s)})$ of $\mathfrak{H}^{(s)}$ by $\mathfrak{A}$. By Lemma 3.1, we have

$$(\mathfrak{A}\mathfrak{G}^{(s)})^\wedge \to \hat{\mathfrak{A}} \to (\mathfrak{A}\mathfrak{G}^{(s)})' \cap \mathfrak{A})^\wedge \to 1 ,$$

therefore we have

$$(\mathfrak{A}\mathfrak{G}^{(s)})^\wedge \to \hat{\mathfrak{A}} \to (\mathfrak{G}^{(s+1)} \cap \mathfrak{A})^\wedge \to 1 .$$

Since $\partial_s \circ \tau_C$ is the transgression mapping corresponding to $(\mathfrak{A}\mathfrak{G}^{(s)}, \pi|\mathfrak{A}\mathfrak{G}^{(s)})$, we have also

$$(\mathfrak{A}\mathfrak{G}^{(s)})^\wedge \to \hat{\mathfrak{A}} \xrightarrow{\partial_s \circ \tau_C} \mathfrak{M}(\mathfrak{H}^{(s)}) .$$

The above two exact sequences imply 1). When $s=0$, these sequences imply also 2). q.e.d.

We denote by $\mathrm{H}^2_s(\mathfrak{H}, \mathfrak{A})$ the subgroup of $\mathrm{H}^2(\mathfrak{H}, \mathfrak{A})$ consisting of all cohomology classes associated to central group extensions of s-type. Now let $(\mathfrak{G}, \pi)$ be a central group extension of $\mathfrak{H}$ by $\mathfrak{A}$ and suppose that $\mathfrak{H}^{(s+1)} = \{I\}$. Then $(\mathfrak{G}, \pi)$ is of s-type if and only if $\mathfrak{G}^{(s+1)} = \{I\}$. In particular, we have[18]

$$\mathrm{H}^2_0(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}) = \mathrm{H}^2_{\mathrm{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}) . \tag{15}$$

PROPOSITION 3.4. *By the natural homomorphism, we have*

$$\mathrm{H}^2_s(\mathfrak{H}/\mathfrak{H}^{(s+1)}, \mathfrak{A}) \cong \mathrm{H}^2_s(\mathfrak{H}, \mathfrak{A}) \qquad \textit{for any } s \geqq 0.$$

PROOF. Let $\bar{C} \in \mathrm{H}^2_s(\mathfrak{H}/\mathfrak{H}^{(s+1)}, \mathfrak{A})$ and $(\bar{\mathfrak{G}}, \bar{\pi})$ a central group extension of $\mathfrak{H}/\mathfrak{H}^{(s+1)}$ by $\mathfrak{A}$ to which $\bar{C}$ is associated. Then, as stated above, we have $\bar{\mathfrak{G}}^{(s+1)} = \{I\}$. Let $C \in \mathrm{H}^2(\mathfrak{H}, \mathfrak{A})$ be corresponding to $\bar{C}$ by the natural mapping and $(\mathfrak{G}, \pi)$ a central group extension of $\mathfrak{H}$ by $\mathfrak{A}$ to which C is associated. Then there exists a homomorphism $\varphi : \mathfrak{G} \to \bar{\mathfrak{G}}$ such that the following diagram is commutative.

17) $\mathfrak{G}'$ is the commutator subgroup of $\mathfrak{G}$.

18) Cf. footnote 12).

$$\begin{tikzcd} 1 \arrow[r] & \mathfrak{A} \arrow[r] \arrow[d] & \mathfrak{G} \arrow[r, "\pi"] \arrow[d, "\varphi"] & \mathfrak{H} \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & \mathfrak{A} \arrow[r] & \bar{\mathfrak{G}} \arrow[r, "\bar{\pi}"'] & \mathfrak{H}/\mathfrak{H}^{(s+1)} \arrow[r] & 1 \end{tikzcd}$$

Since $\bar{\mathfrak{G}}^{(s+1)} \cap \mathfrak{A} = \varphi(\mathfrak{G}^{(s+1)} \cap \mathfrak{A}) \subset \bar{\mathfrak{G}}^{(s+1)} = \{I\}$, it follows from Proposition 3.3 that $(\bar{\mathfrak{G}}, \bar{\pi})$ is of s-type. Thus we obtain the natural homomorphism

$$\mathrm{H}_s^2(\mathfrak{H}/\mathfrak{H}^{(s+1)}, \mathfrak{A}) \to \mathrm{H}_s^2(\mathfrak{H}, \mathfrak{A}) . \tag{16}$$

Now suppose that $(\mathfrak{G}, \pi)$ splits. Then there exists a homomorphism $\psi : \mathfrak{H} \to \mathfrak{G}$ such that $\pi \circ \psi = 1$. Also we have

$$(\varphi \circ \psi)(\mathfrak{H}^{(s+1)}) \subset \varphi(\mathfrak{G}^{(s+1)}) \subset \bar{\mathfrak{G}}^{(s+1)} = \{I\} .$$

Therefore $\varphi \circ \psi$ induces a homomorphism $\bar{\psi} : \mathfrak{H}/\mathfrak{H}^{(s+1)} \to \bar{\mathfrak{G}}$ such that $\bar{\pi} \circ \bar{\psi} = 1$ whence $(\bar{\mathfrak{G}}, \bar{\pi})$ also splits. This proves that (16) is injective. We take any $C \in \mathrm{H}_s^2(\mathfrak{H}, \mathfrak{A})$ and let $(\mathfrak{G}, \pi)$ be a central group extension to which C is associated. We take the factor group $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{G}^{(s+1)}$ and the natural homomorphism $\bar{\pi} : \bar{\mathfrak{G}} \to \mathfrak{H}/\mathfrak{H}^{(s+1)}$. We easily see that the kernel of $\bar{\pi}$ is isomorphic to $\mathfrak{A}$ naturally since $\mathfrak{G}^{(s+1)} \cap \mathfrak{A} = \{I\}$ by Proposition 3.3; we identify these groups. Then the cohomology class $\bar{C}$ associated to $(\bar{\mathfrak{G}}, \bar{\pi})$ is in $\mathrm{H}_s^2(\mathfrak{H}/\mathfrak{H}^{(s+1)}, \mathfrak{A})$ and mapped to C by (16). This completes the proof.

From (15) and Proposition 3.4, it follows that

$$\mathrm{H}_{\mathrm{abel}}^2(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}) \cong \mathrm{H}_0^2(\mathfrak{H}, \mathfrak{A}) \tag{17}$$

by the natural homomorphism.

3.3. A fundamental exact sequence and its applications.

Let $\mathfrak{H}, \mathfrak{A}, K, \hat{\mathfrak{A}}$ and $\mathfrak{M}(\mathfrak{H})$ be as stated in § 3.2. Then the following theorem is fundamental.

THEOREM 3.1. *Let $\mathfrak{H}$ be a finite group and $\mathfrak{A}$ a finite abelian group. Then we have the splitting exact sequence*

$$1 \to \mathrm{H}_{\mathrm{abel}}^2(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}) \to \mathrm{H}^2(\mathfrak{H}, \mathfrak{A}) \to \mathrm{Hom}\,(\hat{\mathfrak{A}}, \mathfrak{M}(\mathfrak{H})) \to 1$$

defined by the natural homomorphisms.

PROOF. By (17), it is sufficient to prove that the homomorphism

$$\mathrm{H}^2(\mathfrak{H}, \mathfrak{A}) \to \mathrm{Hom}\,(\hat{\mathfrak{A}}, \mathfrak{M}(\mathfrak{H}))$$

is surjective and its kernel $\mathrm{H}_0^2(\mathfrak{H}, \mathfrak{A})$ splits.[19] We need the following lemma for $n=2$.

19) This fact holds for any $n>0$ if we set $\mathfrak{M}(\mathfrak{H}) = \mathrm{H}^n(\mathfrak{H}, K^*)$.

LEMMA 3.2. *Let* $\mathfrak{H}$ *be a group and* $\tilde{\mathfrak{A}}$, Ω *be abelian groups. For any n-cochain* $f\in C^n(\mathfrak{H}, \mathrm{Hom}(\tilde{\mathfrak{A}}, \Omega))$, *we define a homomorphism* $\varphi\in \mathrm{Hom}(\tilde{\mathfrak{A}}, C^n(\mathfrak{H}, \Omega))$ *by the formula*

$$(\varphi(A))(X_1, \cdots, X_n)=(f(X_1, \cdots, X_n))(A) \qquad (A\in\tilde{\mathfrak{A}};\ X_1, \cdots, X_n\in\mathfrak{H}).$$

Then the mapping $f\to\varphi$ *is a bijection and induces naturally a bijection*

$$Z^n(\mathfrak{H}, \mathrm{Hom}(\tilde{\mathfrak{A}}, \Omega))\to \mathrm{Hom}(\tilde{\mathfrak{A}}, Z^n(\mathfrak{H}, \Omega))$$

and an injection

$$B^n(\mathfrak{H}, \mathrm{Hom}(\tilde{\mathfrak{A}}, \Omega))\to \mathrm{Hom}(\tilde{\mathfrak{A}}, B^n(\mathfrak{H}, \Omega)).$$

PROOF. Straightforward.

Now we set $\Omega=K^*$ and $\tilde{\mathfrak{A}}=\hat{\mathfrak{A}}$ in the above lemma. Then we have the following bijection and injection, since $\mathfrak{A}\cong\mathrm{Hom}(\hat{\mathfrak{A}}, K^*)$ naturally.

$$(18)\qquad \begin{aligned} &1\to Z^2(\mathfrak{H}, \mathfrak{A})\to \mathrm{Hom}(\hat{\mathfrak{A}}, Z^2(\mathfrak{H}, K^*))\to 1\,, \\ &1\to B^2(\mathfrak{H}, \mathfrak{A})\to \mathrm{Hom}(\hat{\mathfrak{A}}, B^2(\mathfrak{H}, K^*))\,. \end{aligned}$$

Moreover, by Proposition 3.1 3) and (4) in § 1.1, we have the splitting exact sequence

$$(19)\qquad 1\to \mathrm{Hom}(\hat{\mathfrak{A}}, B^2(\mathfrak{H}, K^*))\to \mathrm{Hom}(\hat{\mathfrak{A}}, Z^2(\mathfrak{H}, K^*))\to \mathrm{Hom}(\hat{\mathfrak{A}}, H^2(\mathfrak{H}, K^*))\to 1\,.$$

Therefore the natural homomorphism

$$H^2(\mathfrak{H}, \mathfrak{A})\to \mathrm{Hom}(\hat{\mathfrak{A}}, H^2(\mathfrak{H}, K^*))$$

induced by (18) and (19), is surjective and its kernel splits. This completes the proof of Theorem 3.1.

Now we shall give some applications of the above theorem. We recall the assumptions on $\mathfrak{H}, \mathfrak{A}, K$ (§ 3.2.). By Theorem 3.1, we have the surjection

$$H^2(\mathfrak{H}, \mathfrak{A})\to \mathrm{Hom}(\mathfrak{A}, \mathfrak{M}(\mathfrak{H}))$$

defined by the homomorphism $C\to\tau_C$. Also we have $\mathfrak{A}\cong\hat{\mathfrak{A}}$. Therefore the followings are clear.

1) There exists a central group extension of bijective type of $\mathfrak{H}$ by $\mathfrak{A}$ if and only if $\mathfrak{A}$ is isomorphic to $\mathfrak{M}(\mathfrak{H})$.

2) There exists a central group extension of surjective type of $\mathfrak{H}$ by $\mathfrak{A}$ if and only if $\mathfrak{A}$ has a subgroup isomorphic to $\mathfrak{M}(\mathfrak{H})$.

3) There exists a central group extension of injective type of $\mathfrak{H}$ by $\mathfrak{A}$ if and only if $\mathfrak{A}$ is isomorphic to a subgroup of $\mathfrak{M}(\mathfrak{H})$.

COROLLARY 1. (Schur [1]) *Let $\mathfrak{H}$ be a finite group of order h and K an h-divisible field. Then there exists a (finite) representation-group of $\mathfrak{H}$* over K.

PROOF. By Proposition 3.1, $\mathfrak{M}(\mathfrak{H})=H^2(\mathfrak{H}, K^*)$ is a finite abelian group. Moreover, by Proposition 1.1 and h-divisibility of K, K is $\mathfrak{M}(\mathfrak{H})$-cyclic (Cf. § 3.2 for the definition.). Hence the Corollary follows from the above 1).

COROLLARY 2. (Schur [2]) *Let $\mathfrak{H}$ and K be as in Corollary* 1. *Then the number of equivalent classes of all representation-groups is equal to*

$$\prod_{i,j}(\varepsilon_i, \eta_j)$$

where $\{\varepsilon_i\}$ and $\{\eta_j\}$ are the invariants of $\mathfrak{H}/\mathfrak{H}'$ and $\mathfrak{M}(\mathfrak{H})$ respectively.

PROOF. First, we fix the kernel $\mathfrak{A}$ of central group extensions of bijective type which is isomorphic to $\mathfrak{M}(\mathfrak{H})$. Then, by Theorem 3.1, the number of strong equivalence classes of those group extensions (Cf. § 1.3.) is equal to

$$[H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}):1][\mathrm{Aut}(\mathfrak{A}):1]$$

where $\mathrm{Aut}(\mathfrak{A})$ is the group of all automorphisms of $\mathfrak{A}$. Now, when we do not fix the kernel $\mathfrak{A}$, the equivalence relation among group extensions of bijective type is weakened modulo $\mathrm{Aut}(\mathfrak{A})\cong \mathrm{Aut}(\mathfrak{M}(\mathfrak{H}))$. Therefore the number of equivalence classes of group extensions of bijective type i.e. representation-groups is equal to the order of $H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{M}(\mathfrak{H}))$. Hence the Corollary follows from Proposition 2.1.

Corollary 1 to Theorem 3.1 is generalized as follows.

PROPOSITION 3.5. *Let $\mathfrak{H}, \mathfrak{A}, K$ be as* in § 3.2. *Let $(\mathfrak{G}, \pi)$ be a central group extension of injective type of $\mathfrak{H}$ by $\mathfrak{A}$. Then there exists a central group extension $(\tilde{\mathfrak{G}}, \tilde{\pi})$ of $\mathfrak{G}$ such that $(\tilde{\mathfrak{G}}, \pi\circ\tilde{\pi})$ is a central group extension of bijective type of $\mathfrak{H}$.*

PROOF. Let $C\in H^2(\mathfrak{H}, \mathfrak{A})$ be the cohomology class associated $(\mathfrak{G}, \pi)$. Then $\tau_C:\hat{\mathfrak{A}}\to\mathfrak{M}(\mathfrak{H})$ is injective. Hence there exists an abelian group extension $\mathfrak{B}$ of $\mathfrak{A}$ and an isomorphism

$$\varphi:\hat{\mathfrak{B}}\to\mathfrak{M}(\mathfrak{H})$$

whose restriction to $\hat{\mathfrak{A}}$ coincides with τ_C. Then we have the following commutative diagram by the natural mappings.

$$\begin{array}{ccccccccc}
1 & \to & H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{B}) & \to & H^2(\mathfrak{H}, \mathfrak{B}) & \to & \mathrm{Hom}(\hat{\mathfrak{B}}, \mathfrak{M}(\mathfrak{H})) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{A}) & \to & H^2(\mathfrak{H}, \mathfrak{A}) & \to & \mathrm{Hom}(\hat{\mathfrak{A}}, \mathfrak{M}(\mathfrak{H})) & \to & 1
\end{array}$$

By Theorem 3.1, the horizontal sequences are exact. It is easily seen that $H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{B})\to H^2_{\text{abel}}(\mathfrak{H}/\mathfrak{H}', \mathfrak{A})$ is surjective since $\mathfrak{B}\to\mathfrak{A}$ is surjective. Therefore it follows easily that there exists a cohomology class $\tilde{C}\in H^2(\mathfrak{H}, \mathfrak{B})$ which is mapped to C. It is sufficient to take a group extension to which $\tilde{C}$ is associated. q.e.d.

§ 4. Ring extensions of a finite group over a field.

4.1. Definition of ring extensions.

Let K be an arbitrary field. By a *ring over* K, we mean a ring $\mathcal{A}$ containing K as a subring and such that the unit element 1 of K is also the unit element of $\mathcal{A}$. However it should be noted that we do not assume that K is contained in the center of $\mathcal{A}$. Let $\mathfrak{H}$ be a finite group. By a *ring extension of* $\mathfrak{H}$ *over* K, we mean an object consisting of a ring $\mathcal{A}$ over K and a direct sum decomposition

$$\mathcal{A} = \sum_{H\in\mathfrak{H}} \mathcal{A}_H$$

of $\mathcal{A}$ into a family of submodules $\mathcal{A}_H$, indexed by $\mathfrak{H}$, such that

R1) $\mathcal{A}_H = Ke_H = e_H K$ for some $e_H \neq 0$ (for any $H\in\mathfrak{H}$),

R2) $\mathcal{A}_P \mathcal{A}_Q = \mathcal{A}_{PQ}$ (for any $P, Q\in\mathfrak{H}$);

the direct sum decomposition $\mathcal{A} = \sum_{H\in\mathfrak{H}} \mathcal{A}_H$ will be called a *structure of ring extension* on $\mathcal{A}$.

Two ring extensions $\mathcal{A} = \sum_{H\in\mathfrak{H}} \mathcal{A}_H$ and $\mathcal{B} = \sum_{H\in\mathfrak{H}} \mathcal{B}_H$ of $\mathfrak{H}$ over K are said to be *isomorphic* if there is a ring isomorphism of $\mathcal{A}$ onto $\mathcal{B}$ such that $\mathcal{A}_H \to \mathcal{B}_H$ $(H\in\mathfrak{H})$.

Let us show some elementary properties on ring extensions. We denote by $\mathcal{A}_H^*$ the set of all non-zero elements in $\mathcal{A}_H$. First we note R1) is also valid for any $e_H \in \mathcal{A}_H^*$ $(H\in\mathfrak{H})$, and $\{e_H\}_{H\in\mathfrak{H}}$ is a left and right K-base of $\mathcal{A}$. This shows that

$$\mathcal{A}_P^* \mathcal{A}_Q^* = \mathcal{A}_{PQ}^* \qquad (P, Q\in\mathfrak{H}). \tag{20}$$

Now we write

$$1 = \sum_{H\in\mathfrak{H}} a_H \qquad (a_H \in \mathcal{A}_H),$$

then we have $a_P \neq 0$ for some $P\in\mathfrak{H}$. Hence $a_P = \sum_{H\in\mathfrak{H}} a_H a_P$. Since $a_H a_P \in \mathcal{A}_{HP}$, we have $a_H a_P = 0$ for any $H \neq I$ where I is the unit element of $\mathfrak{H}$. Hence $a_H = 0$ for any $H \neq I$ by (20). Thus we have $1 = a_I \in \mathcal{A}_I$, which shows

$$\mathcal{A}_I = K. \tag{21}$$

Let $\mathfrak{G}$ be the disjoint union of $\mathcal{A}_H^*$ $(H\in\mathfrak{H})$. From (20) and (21), it follows that $\mathfrak{G}$ is a group containing the group $\mathcal{A}_I^* = K^*$ under the multiplication in $\mathcal{A}$. Let π be the natural homomorphism $\mathfrak{G} \to \mathfrak{H}$. Then $(\mathfrak{G}, \pi)$ is a group extension of $\mathfrak{H}$ by K^*; we call this the group extension associated with the ring extension $\mathcal{A} = \sum_{H\in\mathfrak{H}} \mathcal{A}_H$. $\mathcal{A}_H^*$ is a coset of $\mathfrak{G}$ modulo K^* corresponding to $H\in\mathfrak{H}$, and $e_H \in \mathcal{A}_H^*$ yields an automorphism of the field K

$$\sigma_H : \lambda \to e_H \lambda e_H^{-1} \quad (e_H \in \mathcal{A}_H^*)$$

which does not depend on the choice of e_H in $\mathcal{A}_H^*$; we denote by ${}^H\lambda$ the element $\sigma_H(\lambda)\in K$ for $\lambda\in K$. The mapping

$$\sigma : H \to \sigma_H$$

is a homomorphism of $\mathfrak{H}$ into the group of automorphisms of the field K, that is, $\mathfrak{H}$ acts on K. We shall say that the ring extension $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ *belongs to* the action σ. The group extension

$$1 \to K^* \to \mathfrak{G} \to \mathfrak{H} \to 1$$

determines a cohomology class in $\mathrm{H}^2_\sigma(\mathfrak{H}, K^*)$.[20] More explicitly, we take a function f of two variables on $\mathfrak{H}$:

$$f(P, Q) = e_P\, e_Q\, e_{PQ}^{-1} \qquad (P, Q\in\mathfrak{H}).$$

Then f is in $\mathrm{Z}^2(\mathfrak{H}, K^*)$ and its cohomology class c does not depend on the choice of $e_H\in\mathcal{A}_H^*$. Moreover isomorphic ring extensions determine the same cohomology class. Thus we obtain a correspondence between isomorphic classes of ring extensions of $\mathfrak{H}$ over K belonging to σ and cohomology classes in $\mathrm{H}^2_\sigma(\mathfrak{H}, K^*)$. It can be shown that this correspondence is bijective as follows.

Suppose that $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ and $\mathcal{B}=\sum_{H\in\mathfrak{H}}\mathcal{B}_H$ determine the same cohomology class $c\in\mathrm{H}^2(\mathfrak{H}, K^*)$. Then we have

$$a_P\, a_Q\, a_{PQ}^{-1} = b_P\, b_Q\, b_{PQ}^{-1} \qquad (P, Q\in\mathfrak{H})$$

for some $a_H\in\mathcal{A}_H^*$ and $b_H\in\mathcal{B}_H^*$ $(H\in\mathfrak{H})$. So we define a mapping φ of $\mathcal{A}$ into $\mathcal{B}$ as follows.

$$\varphi(\sum_{H\in\mathfrak{H}}\lambda_H\, a_H)=\sum_{H\in\mathfrak{H}}\lambda_H\, b_H \qquad (\lambda_H\in K)$$

It is easily seen that φ is a ring isomorphism and $\varphi(\mathcal{A}_H)=\mathcal{B}_H$ $(H\in\mathfrak{H})$, therefore $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ and $\mathcal{B}=\sum_{H\in\mathfrak{H}}\mathcal{B}_H$ are isomorphic. Next let us construct a ring extension corresponding to any cohomology class $c\in\mathrm{H}^2(\mathfrak{H}, K^*)$.[21] We take a family $\{u_H\}_{H\in\mathfrak{H}}$ of indeterminates indexed by $\mathfrak{H}$. Let $\mathcal{A}$ be a left vector space over K such that $\{u_H\}_{H\in\mathfrak{H}}$ is a base of $\mathcal{A}$. Then we have a direct sum decomposition $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ where $\mathcal{A}_H=K\,u_H$ $(H\in\mathfrak{H})$. Now we introduce a law of multiplication into $\mathcal{A}$. Let f be a normalized cocycle in c, and we define the multiplication as follows.

$$(\sum_{P\in\mathfrak{H}}\lambda_P u_P)(\sum_{Q\in\mathfrak{H}}\mu_Q\, u_Q) = \sum_{P,\,Q\in\mathfrak{H}}\lambda_P\, {}^P\mu_Q\, f(P, Q)\, u_{PQ}$$

20) σ induces an action of $\mathfrak{H}$ on K^*; we denote it by the same symbol σ. $\mathrm{H}^2_\sigma(\mathfrak{H}, K^*)$ means the cohomology group w.r.t. this action σ.

21) When σ is faithful, an intrinsic construction by a group extension is given in [Serre, Théorie des algèbres simples, Sem. de top. alg. (1950–1951)]. Also cf. [6], [7], [8], [9].

The distributivity is clear. The associativity follows from the condition of cocycle. Thus $\mathcal{A}$ becomes a ring. Clearly Ku_I is a subring of $\mathcal{A}$, and isomorphic to K by the mapping $\lambda \to \lambda u_I$ since $f(I,I)=1$; we identify λ with λu_I, hence $1=u_I$. Then $\mathcal{A}$ is a ring over K and we have $\mathcal{A}_H=Ku_H=u_H K$ and $\mathcal{A}_P\mathcal{A}_Q=\mathcal{A}_{PQ}$ $(H,P,Q\in\mathfrak{H})$. Hence $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ is a ring extension of $\mathfrak{H}$ over K. It is easily seen that this ring extension corresponds to the given cohomology class c. This completes the bijective correspondence between all isomorphic classes of ring extensions of $\mathfrak{H}$ over K belonging to σ and all cohomology classes in $\mathrm{H}^2_\sigma(\mathfrak{H},K^*)$.

Let σ be an action of $\mathfrak{H}$ on K i.e. an homomorphism of $\mathfrak{H}$ into the group of automorphisms of K. Let $\mathfrak{H}_0$ be the kernel of σ i.e.

$$\mathfrak{H}_0=\{H\in\mathfrak{H};\ {}^H\lambda=\lambda \quad \text{for all } \lambda\in K\},$$

and k be the fixed subfield of $\mathfrak{H}$ i.e.

$$k=\{\lambda\in K;\ {}^H\lambda=\lambda \quad \text{for all } H\in\mathfrak{H}\}.$$

Then K is a Galois extension of k whose Galois group is isomorphic to $\mathfrak{H}/\mathfrak{H}_0$. Any ring extension belonging to σ is an algebra over k of rank $[\mathfrak{H}:I][\mathfrak{H}:\mathfrak{H}_0]$.

When σ is faithful i.e. the mapping $H\to\sigma_H$ is injective, we have $\mathfrak{H}_0=\{I\}$ and can identify $\mathfrak{H}$ with the Galois group of K over k. In this case, the ring extension is noting but the *crossed product* of $\mathfrak{H}$ with K. On the contrary, when σ is trivial i.e. $\mathfrak{H}$ acts on K trivially, we have $K=k$ and call a ring extension $\mathcal{A}$ an *algebra extension* of $\mathfrak{H}$ over K. Especially, if the cohomology class corresponding to $\mathcal{A}$ is trivial, we obtain the *group algebra* of $\mathfrak{H}$ over K by taking a base $\{e_H\}_{H\in\mathfrak{H}}$ such that $e_P e_Q=e_{PQ}$ $(P,Q\in\mathfrak{H})$.

4.2. Semi-simplicity.

Let $\mathfrak{H},\sigma,K$ and $\mathfrak{H}_0$ be as in §4.1. With a ring extension $\mathcal{A}=\sum_{H\in\mathfrak{H}}\mathcal{A}_H$ belonging to σ is associated a subring $\mathcal{A}_0$ defined by

$$\mathcal{A}_0=\sum_{H\in\mathfrak{H}_0}\mathcal{A}_H.$$

The ring $\mathcal{A}_0$ and the above direct sum decomposition constitute an algebra extension of $\mathfrak{H}_0$ over K. This algebra extension is called the *restriction* of the ring extension $\mathcal{A}$ to $\mathfrak{H}_0$.

LEMMA 4.1. *If $\mathcal{J}$ is a non-zero ideal of $\mathcal{A}$, then $\mathcal{J}\cap\mathcal{A}_0$ is also a non-zero ideal of $\mathcal{A}_0$.*

PROOF. For each element $a=\sum_{H\in\mathfrak{H}}a_H$ $(a_H\in\mathcal{A}_H)$, we set $\mathfrak{S}(a)=\{H\in\mathfrak{H};\ a_H\neq 0\}$.

Clearly $\mathfrak{S}(a)$ is empty if and only if $a=0$. We take a non-zero element a of $\mathfrak{J}$ such that $\mathfrak{S}(a)$ is minimal among $\{\mathfrak{S}(x)\}_{0\neq x\in\mathfrak{J}}$. Then we can prove that $\mathfrak{S}(a)$ is contained in a certain coset of $\mathfrak{H}$ modulo $\mathfrak{H}_0$. In fact, suppose that there exist two elements P, Q in $\mathfrak{S}(a)$ such that $P^{-1}Q\notin\mathfrak{H}_0$. Then, by the definition of $\mathfrak{H}_0$, there exists an element λ in K such that $\lambda\neq{}^{P^{-1}Q}\lambda$, whence ${}^{P}\lambda\neq{}^{Q}\lambda$. Since $\mathfrak{J}$ is an ideal containing a, the element $b={}^{P}\lambda a-a\lambda=\sum_{H\in\mathfrak{H}}({}^{P}\lambda a_H-a_H\lambda)$ is contained in $\mathfrak{J}$. However we have ${}^{P}\lambda a_P-a_P\lambda=0$, ${}^{P}\lambda a_Q-a_Q\lambda=({}^{P}\lambda-{}^{Q}\lambda)\,a_Q\neq0$. Therefore $\mathfrak{S}(a)\supsetneqq\mathfrak{S}(b)\neq\phi$. This contradicts the minimality of $\mathfrak{S}(a)$, and thus $\mathfrak{S}(a)$ is contained in a certain coset $H\mathfrak{H}_0$. If we take an element $e\in\mathcal{A}^*_{H^{-1}}$, we have $\mathfrak{J}\ni ea\neq0$, and $\mathfrak{S}(ea)\subset\mathfrak{H}_0$. Therefore $\mathfrak{J}\cap\mathcal{A}_0\ni ea\neq0$. This completes the proof.

The above lemma implies that if $\mathcal{A}_0$ is simple then $\mathcal{A}$ is simple (Theorem 4.2 1)). More generally we have the following theorem.

THEOREM 4.1. *Let $\mathcal{A}$ be a ring extension of a finite group $\mathfrak{H}$ over a field K, and $\mathfrak{H}_0$ be the kernel of the corresponding action. If the characteristic of K does not divide the order of $\mathfrak{H}_0$, then $\mathcal{A}$ is semi-simple.*

PROOF. If $\mathcal{A}$ has the non-zero radical $\mathfrak{R}$, $\mathfrak{R}\cap\mathcal{A}_0$ is a non-zero nilpotent ideal in $\mathcal{A}_0$ by Lemma 4.1. Hence it is sufficient to prove that $\mathcal{A}_0$ is semi-simple. So we can assume that $\mathfrak{H}$ acts on trivially, whence $\mathcal{A}$ is an algebra extension of $\mathfrak{H}$ over K, and the characteristic of K does not divide the order of $\mathfrak{H}$. Let ψ be the character (i.e. the trace function) of the regular representation of $\mathcal{A}$ over K. We take $e_I=1$, $e_H\in\mathcal{A}^*_H$ $(H\in\mathfrak{H})$, and set $f(P,Q)=e_P e_Q e_{PQ}^{-1}$. Then the discriminant D of $\mathcal{A}$ w.r.t. the base $\{e_H\}_{H\in\mathfrak{H}}$ is computed as follows.

$$\begin{aligned}D&=\det(\psi(e_P e_Q))=\det(f(P,Q)\psi(e_{PQ}))\\&=\det(f(P,Q)\,h\,\delta_{P^{-1},Q})=h^h\operatorname{sgn}\begin{pmatrix}P\\P^{-1}\end{pmatrix}\prod_{P\in\mathfrak{H}}f(P,P^{-1})\neq0\,,\end{aligned}$$

where h is the order of $\mathfrak{H}$. Therefore $\mathcal{A}$ is semi-simple.

4.3. The center.

Let $\mathfrak{H}, \mathfrak{H}_0, \sigma, K, \mathcal{A}$ and $\mathcal{A}_0$ be as in § 4.2.

LEMMA 4.2. *The center of $\mathcal{A}$ is contained in the center of $\mathcal{A}_0$.*

PROOF. Let $a=\sum_{H\in\mathfrak{H}}a_H$ $(a_H\in\mathcal{A}_H)$ be in the center of $\mathcal{A}$. It follows that $\sum_{H\in\mathfrak{H}}\lambda a_H=\sum_{H\in\mathfrak{H}}a_H\lambda=\sum_{H\in\mathfrak{H}}{}^{H}\lambda\,a_H$ for all $\lambda\in K$. Therefore we have

$$\lambda a_H={}^{H}\lambda\,a_H\qquad\text{for all } H\in\mathfrak{H},\ \lambda\in K. \tag{22}$$

Let H be any element of $\mathfrak{H}$ not contained in $\mathfrak{H}_0$. Then $\lambda\neq{}^{H}\lambda$ for some $\lambda\in K$. Therefore, from (22), we have $a_H=0$ for $H\notin\mathfrak{H}_0$, whence $a\in\mathcal{A}_0$. This completes the proof.

THEOREM 4.2. *Let $\mathcal{A}$ be a ring extension of a finite group $\mathfrak{H}$ over a field K, k be the fixed field of $\mathfrak{H}$, and $\mathcal{A}_0$ be the restriction of $\mathcal{A}$ to the kernel $\mathfrak{H}_0$ of the corresponding action. Then we have*

1) *If $\mathcal{A}_0$ is simple, then $\mathcal{A}$ is simple.*

2) *If the center of $\mathcal{A}_0$ is K, then the center of $\mathcal{A}$ is k.*

PROOF. 1) It follows immediately from Lemma 4.1.

2) From the assumption and Lemma 4.2, it follows that the center of $\mathcal{A}$ is contained in K. Let λ be any element of the center of $\mathcal{A}$ contained in K. We have $\lambda e_H = e_H \lambda = {}^H\lambda e_H$ for $e_H \in \mathcal{A}_H^*$ $(H \in \mathfrak{H})$, whence $\lambda \in k$. This completes the proof.

COROLLARY. *Let $\mathcal{A}$ be a ring extension of a finite group $\mathfrak{H}$ over a field K. If the corresponding action is faithful, then $\mathcal{A}$ is central simple over the fixed field of the action.*

PROOF. In this case, we have $\mathcal{A}_0 = K$. Therefore the corollary follows from the theorem.

This corollary is well known, and $\mathcal{A}$ is of rank $[\mathfrak{H} : I]^2$ over k. In the following we shall study the center of a ring extension in detail.

Let $\mathcal{A}$ be a ring extension of a finite group $\mathfrak{H}$ over K and c the corresponding cohomology class in $\mathrm{H}^2_\sigma(\mathfrak{H}, K^*)$ where σ is the action corresponding to $\mathcal{A}$. If the action of an element P in $\mathfrak{H}$ is trivial i.e. $P \in \mathfrak{H}_0$, we have the homomorphism

$$\mathrm{H}^2_\sigma(\mathfrak{H}, K^*) \to \mathrm{H}^1_\sigma(\mathfrak{Z}_P, K^*)$$

where $\mathfrak{Z}_P$ is the centralizer of P in $\mathfrak{H}$, as stated in § 2.1; we denote by c_P the image of c under this homomorphism. We call P to be *$\mathcal{A}$-normal* or *c-normal* if $c_P = 1$. We take a cocycle f in c and define $f_P \in \mathrm{C}^1(\mathfrak{H}, K^*)$ by (7) in § 2.1. Then an element P in $\mathfrak{H}$ is $\mathcal{A}$-normal if and only if P is in $\mathfrak{H}_0$ and there exists an element $\alpha_P \in K^*$ such that

$$f_P(X) = {}^X\alpha_P \alpha_P^{-1} \qquad \text{for all } X \in \mathfrak{Z}_P. \tag{23}$$

LEMMA 4.3. *Let P and Q be two conjugate elements of $\mathfrak{H}$. If P is $\mathcal{A}$-normal, then Q is also $\mathcal{A}$-normal.*

PROOF. Let $Q = H^{-1}PH$ for some $H \in \mathfrak{H}$ and P an $\mathcal{A}$-normal element. Then we have $Q \in \mathfrak{H}_0$ and $\mathfrak{Z}_Q = H^{-1}\mathfrak{Z}_P H$, where $\mathfrak{Z}_Q$ is the centralizer of Q in $\mathfrak{H}$. Hence, for any $Y \in \mathfrak{Z}_Q$, we have $X = HYH^{-1} \in \mathfrak{Z}_P$ and by (8) in § 2.1,

$$\begin{aligned} {}^H f_Q(Y) &= {}^H f_{H^{-1}PH}(Y) = f_P(HY) f_P(H)^{-1} = f_P(XH) f_P(H)^{-1} \\ &= {}^X f_P(H) f_P(X) f_P(H)^{-1}. \end{aligned}$$

This implies, by (23),

$${}^H f_Q(Y) = {}^X f_P(H)\, {}^X\alpha_P \alpha_P^{-1} f_P(H)^{-1}.$$

We set $\alpha_Q={}^{H^{-1}}(\alpha_P f_P(H))$. Then we have easily

$$f_Q(Y)={}^{Y}\alpha_Q\alpha_Q^{-1}\qquad \text{for all } Y\in\mathfrak{Z}_Q,$$

whence Q is $\mathcal{A}$-normal. q.e.d.

We call a conjugate class $\mathfrak{C}$ of $\mathfrak{H}$ *$\mathcal{A}$-normal*, if $\mathfrak{C}$ contains an $\mathcal{A}$-normal element, or equivalently, if all elements of $\mathfrak{C}$ are $\mathcal{A}$-normal.

THEOREM 4.3.[22] *Let $\mathcal{A}$ be a ring extension of a finite group $\mathfrak{H}$ over a field K and $\mathcal{Z}(\mathcal{A})$ be the center of $\mathcal{A}$. For any $\mathcal{A}$-normal conjugate class $\mathfrak{C}$ of $\mathfrak{H}$, we set*

$$\mathcal{Z}(\mathfrak{C})=\mathcal{Z}(\mathcal{A})\cap\sum_{P\in\mathfrak{C}}\mathcal{A}_P.$$

Then we have

$$\mathcal{Z}(\mathcal{A})=\sum_{\mathfrak{C}}\mathcal{Z}(\mathfrak{C})$$

where $\mathfrak{C}$ runs over all $\mathcal{A}$-normal conjugate classes of $\mathfrak{H}$. Furthermore we have

$$[\mathcal{Z}(\mathfrak{C}):k]=[K_P:k]\qquad (P\in\mathfrak{C})$$

where k is the fixed field of $\mathfrak{H}$ and K_P is the fixed field of the centralizer $\mathfrak{Z}_P$ of P in $\mathfrak{H}$.

PROOF. By Lemma 4.2, we have $\mathcal{Z}(\mathcal{A})\subset\mathcal{A}_0$. We take any element a of $\mathcal{Z}(\mathcal{A})$ and write it in the form

$$a=\sum_{\mathfrak{C}}a_{\mathfrak{C}}$$

where $\mathfrak{C}$ runs over all conjugate classes of $\mathfrak{H}$ contained in $\mathfrak{H}_0$ and $a_{\mathfrak{C}}$ is in $\sum_{P\in\mathfrak{C}}\mathcal{A}_P$. Let e_H be in $\mathcal{A}_H^*$. Since $e_H a e_H^{-1}=a$, we easily see that $e_H a_{\mathfrak{C}} e_H^{-1}=a_{\mathfrak{C}}$ for all e_H, whence $a_{\mathfrak{C}}$ is in $\mathcal{Z}(\mathcal{A})$. This proves that $\mathcal{Z}(\mathcal{A})=\sum_{\mathfrak{C}}\mathcal{Z}(\mathfrak{C})$ where $\mathfrak{C}$ runs all conjugate classes of $\mathfrak{H}$ contained in $\mathfrak{H}_0$.

Let us compute $[\mathcal{Z}(\mathfrak{C}):k]$. Let f be a cocycle corresponding to a base $\{e_H\}_{H\in\mathfrak{H}}$. Then an element $\sum_{P\in\mathfrak{C}}\lambda_P e_P$ is contained in $\mathcal{Z}(\mathfrak{C})$ if and only if

$$\lambda_P f_P(H)={}^{H}\lambda_{H^{-1}PH}\qquad \text{for all } P\in\mathfrak{C} \text{ and } H\in\mathfrak{H}. \tag{24}$$

Now we fix an element P in $\mathfrak{C}$ and consider a k-linear mapping ι of $\mathcal{Z}(\mathfrak{C})$ into K as follows

$$\iota:\sum_{Q\in\mathfrak{C}}\lambda_Q e_Q\longrightarrow\lambda_P.$$

From (24), it follows that the mapping ι is injective. We shall prove that the image of ι coincides with the k-space

22) Cf. [8] for the case of $c=1$.

$$\Lambda_P=\{\lambda\in K\,;\,\lambda f_P(Z)={}^{Z}\lambda \quad \text{for all } Z\in\mathfrak{Z}_P\}\,.$$

The image of ι is contained in Λ_P because of (24). Let $\lambda\neq 0$ be any element of Λ_P and we define

$$\lambda_Q = {}^{X^{-1}}(\lambda f_P(X)) \tag{25}$$

where $Q=X^{-1}PX\in\mathfrak{C}$. We have to show that (25) does not depend on the choice of X. It is sufficient to show that (25) is invariant even if we substitute X by ZX ($Z\in\mathfrak{Z}_P$). From (8) in § 2.1 and the definition of Λ_P, it follows that
$${}^{X^{-1}Z^{-1}}(\lambda f_P(ZX))={}^{X^{-1}Z^{-1}}\lambda\,{}^{X^{-1}}f_P(X)\,{}^{X^{-1}Z^{-1}}f_P(Z)={}^{X^{-1}}({}^{Z^{-1}}(\lambda f_P(Z))\,{}^{X^{-1}}f_P(X)={}^{X^{-1}}(\lambda f_P(X)).$$
This shows that λ_Q is well defined for any $Q\in\mathfrak{C}$. Thus we obtain an element $\sum\limits_{Q\in\mathfrak{C}}\lambda_Q e_Q$. Then we have, for any $Q\in\mathfrak{C}$ and $H\in\mathfrak{H}$,

$$\begin{aligned}{}^{H}\lambda_{H^{-1}QH}&={}^{H}\lambda_{H^{-1}X^{-1}PXH}={}^{H}({}^{H^{-1}X^{-1}}(\lambda f_P(XH))\\&={}^{X^{-1}}(\lambda f_P(XH))={}^{X^{-1}}(\lambda\,{}^{X}f_{X^{-1}PX}(H)\,f_P(X))\\&={}^{X^{-1}}(\lambda f_P(X))\,f_Q(H)=\lambda_Q f_Q(H)\,,\end{aligned}$$

where $Q=X^{-1}PX$. Hence, from (24), the element $\sum\limits_{Q\in\mathfrak{C}}\lambda_Q e_Q$ is contained in $\mathcal{Z}(\mathfrak{C})$ and mapped to $\lambda\in\Lambda_P$ by ι. This completes the k-isomorphism

$$\mathcal{Z}(\mathfrak{C})\cong\Lambda_P\,.$$

Now we compute the dimension of Λ_P over k. If $\mathfrak{C}$ hence P is not $\mathcal{A}$-normal, it follows from (23) that $\Lambda_P=\{0\}$. Let $\mathfrak{C}$ be $\mathcal{A}$-normal. Then there exists a non-zero element $\mu\in\Lambda_P$. An element $\lambda\in K$ is contained in Λ_P if and only if ${}^{Z}(\lambda/\mu)=(\lambda/\mu)$ for all $Z\in\mathfrak{Z}_P$. Therefore we have $\Lambda_P=\mu K_P$ which implies $[\mathcal{Z}(\mathfrak{C}):k]=[\Lambda_P:k]$ $=[K_P:k]$. This completes the proof.

4.4. The case of algebra extensions.

We consider an algebra extension $\mathcal{A}$ of a finite group $\mathfrak{H}$ over a field K. Let f be a 2-cocycle of $\mathfrak{H}$ in K^* corresponding to $\mathcal{A}$. Then an element P in $\mathfrak{H}$ is $\mathcal{A}$-normal if and only if

$$f(P,X)=f(X,P) \qquad \text{for all } X\in\mathfrak{Z}_P$$

where $\mathfrak{Z}_P$ is the centralizer of P in $\mathfrak{H}$. We have, by Theorem 4.3,

COROLLARY. *Let $\mathcal{A}$ be an algebra extension of a finite group $\mathfrak{H}$ over a field K and $\mathcal{Z}(\mathcal{A})$ be the center of $\mathcal{A}$. Then, for any $\mathcal{A}$-normal conjugate class $\mathfrak{C}$ of $\mathfrak{H}$, there exists an elment $e_{\mathfrak{C}}\neq 0$ in $\sum\limits_{P\in\mathfrak{C}}\mathcal{A}_P$ such that*

$$\mathcal{Z}(\mathcal{A})=\sum_{\mathfrak{C}}K e_{\mathfrak{C}}$$

where $\mathfrak{C}$ runs over all $\mathcal{A}$-normal conjugate classes of $\mathfrak{H}$.

From the corollary, it follows that the dimension of $\mathfrak{Z}(\mathcal{A})$ is equal to the number of $\mathcal{A}$-normal conjugate classes of $\mathfrak{H}$. In addition, it can be proved that this number is equal to

$$(1/[\mathfrak{H}:I])\sum_{\substack{PQ=QP\\ P,\,Q\in\mathfrak{H}}} f(P,Q)\,f(Q,P)^{-1}$$

if K is of characteristic 0.[23] In fact, we have

$$\sum_{X\in\mathfrak{Z}_P} f_P(X)=\begin{cases}[\mathfrak{Z}_P:I] & \text{if } P \text{ is } \mathcal{A}\text{-normal,}\\ 0 & \text{otherwise,}\end{cases}$$

since f_P is a homomorphism of $\mathfrak{Z}_P$ into K^*. Therefore we have

$$\sum_{PQ=QP} f(P,Q)\,f(Q,P)^{-1}=\sum_{P\in\mathfrak{H}}\ \sum_{X\in\mathfrak{Z}_P} f_P(X)=\sum_{P:\text{normal}}[\mathfrak{Z}_P:I]$$
$$=\sum_{\mathfrak{C}:\text{normal}}[\mathfrak{H}:\mathfrak{Z}_P][\mathfrak{Z}_P:I]=[\mathfrak{H}:I]\sum_{\mathfrak{C}:\text{normal}}1$$

which completes the proof.

In the following, we assume that $\mathfrak{H}$ is abelian. In this case, any conjugate class of $\mathfrak{H}$ consists of a single element and $\mathfrak{Z}_P=\mathfrak{H}$ for any $P\in\mathfrak{H}$. Let $\mathcal{A}$ be an algebra extension of $\mathfrak{H}$ over a field K, c the corresponding cohomology class and φ the anti-symmetric pairing corresponding to c (Cf. Theorem 2.2.); we shall say that φ corresponds to $\mathcal{A}$. Then an element P in $\mathfrak{H}$ is $\mathcal{A}$-normal if and only if

$$\varphi(P,X)=1 \qquad \text{for all } X\in\mathfrak{H}.$$

Hence the set $\mathfrak{N}$ of all $\mathcal{A}$-normal elements of $\mathfrak{H}$ coincides with the annihilator of φ, whence $\mathfrak{N}$ is a subgroup of $\mathfrak{H}$.

If φ is non-degenerate i.e. $\mathfrak{N}=\{I\}$, then we have an isomorphism of $\mathfrak{H}$ into $\hat{\mathfrak{H}}=\mathrm{Hom}(\mathfrak{H},K^*):H\to\varphi_H$ where $\varphi_H(X)=\varphi(H,X)$. It follows that the characteristic of K does not divide the order of $\mathfrak{H}$. Now we have, by Corollary to Theorem 4.3,

$$\mathfrak{Z}(\mathcal{A})=\sum_{N\in\mathfrak{N}}\mathcal{A}_N\,.$$

Therefore we have, by Theorem 4.1, the following.

PROPOSITION 4.1. *Let $\mathcal{A}$ be an algebra extension of a finite abelian group $\mathfrak{H}$ over a field K, φ be the corresponding anti-symmetric pairing and $\mathfrak{N}$ be the annihilator of φ. Then the center of $\mathcal{A}$ is given as follows.*

$$\mathfrak{Z}(\mathcal{A})=\sum_{N\in\mathfrak{N}}\mathcal{A}_N\,.$$

Moreover $\mathcal{A}$ is central simple if and only if φ is non-degenerate.

In §6, we shall study the structures of algebra extension of abelian groups in detail.

23) This fact was noted by N. Iwahori.

§ 5. Projective representations and modules.

5.1. An equivalence of $\mathcal{A}$-modules.

Let $\mathcal{A}$ be an algebra extension of a finite group $\mathfrak{H}$ over a field K. We consider the finite abelian group $\hat{\mathfrak{H}}=\mathrm{Hom}(\mathfrak{H}, K^*)$. For each $\chi\in\hat{\mathfrak{H}}$, we have an algebra automorphism $\bar{\chi}$ of $\mathcal{A}$ defined by

$$\bar{\chi}(\sum_{H\in\mathfrak{H}} a_H) = \sum_{H\in\mathfrak{H}} \chi(H)\, a_H$$

The mapping $\chi\to\bar{\chi}$ is an injective homomorphism of $\hat{\mathfrak{H}}$ into the group of algebra automorphisms of $\mathcal{A}$ i.e. $\hat{\mathfrak{H}}$ acts on the algebra $\mathcal{A}$ faithfully. Furthermore the $\bar{\chi}$ are linearly independent over K, since the χ are linearly independent over K.

In the following we always assume that $\mathcal{A}$-modules are finite dimensional over K. Two $\mathcal{A}$-modules V_1 and V_2 are called to be *equivalent* if there exist an element $\chi\in\hat{\mathfrak{H}}$ and a K-isomorphism $\varphi: V_1\to V_2$ such that

$$\varphi(a\, v) = \bar{\chi}(a)\varphi(v) \qquad \text{for all } a\in\mathcal{A},\ v\in V_1; \tag{26}$$

we denote by $V_1\sim V_2$. Clearly the relation $\sim$ is an equivalence relation. If V_1 and V_2 are $\mathcal{A}$-isomorphic, then they are equivalent.

By Theorem 4.1, $\mathcal{A}$ is semi-simple if the characteristic of K does not divide the order of $\mathfrak{H}$. So we assume that $\mathcal{A}$ is semi-simple. Then $\mathcal{A}$ is decomposed into the direct sum of all minimal (two-sided) ideals:

$$\mathcal{A}=\mathcal{A}_1+\mathcal{A}_2+\cdots+\mathcal{A}_m\,.$$

Hence we easily see that any $\chi\in\hat{\mathfrak{H}}$ induces a permutation of the set $\{\mathcal{A}_i\}_{1\leq i\leq m}$ i.e. $\hat{\mathfrak{H}}$ acts on $\{\mathcal{A}_i\}_{1\leq i\leq m}$; $\mathcal{A}_i$ and $\mathcal{A}_j$ are called to be *equivalent* if $\bar{\chi}(\mathcal{A}_i)=\mathcal{A}_j$ for some $\chi\in\hat{\mathfrak{H}}$. It is well known that any simple $\mathcal{A}$-module is isomorphic to a minimal left ideal of some $\mathcal{A}_i$ as left $\mathcal{A}$-module. It is easily seen that $\mathcal{A}_i$ and $\mathcal{A}_j$ are equivalent in the above sense if and only if minimal left ideals of $\mathcal{A}_i$ and $\mathcal{A}_j$ are equivalent as $\mathcal{A}$-modules.[24)]

5.2. Representation spaces and $\mathcal{A}$-modules.

Let us consider the relation between the projective representations of a finite group $\mathfrak{H}$ and $\mathcal{A}$-modules where $\mathcal{A}$ is an algebra extension of $\mathfrak{H}$ over a field K. Let c be the cohomology class in $\mathrm{H}^2(\mathfrak{H}, K^*)$ corresponding to $\mathcal{A}$ (Cf. § 4.1.). Let $\mathfrak{M}_{\mathcal{A}}$ be all equivalent classes of $\mathcal{A}$-modules and $\mathfrak{P}_c$ be all equivalent classes of projective representations belonging to c i.e. the inverse image of c under the mapping Ψ_2 (Cf. § 1.4.) In the following, we shall establish a bijective correspondence between $\mathfrak{M}_{\mathcal{A}}$ and P_c.

24) Note that minimal left ideals of $\mathcal{A}_i$ and $\mathcal{A}_j$ are not isomorphic as $\mathcal{A}$-modules if $i\neq j$.

Let V be an $\mathcal{A}$-module. For each $H\in\mathfrak{H}$, we define $T(H)\in \mathrm{GL}(V)$, where V is regarded as a vector space over K, as follows.

$$T(H): v \rightarrow e_H\, v \qquad (e_H\in\mathcal{A}_H^*).$$

The mapping $T: H\rightarrow T(H)$ determines the mapping

$$\rho: \mathfrak{H}\rightarrow \mathrm{PGL}(V)$$

which is independent of the choice of e_H $(H\in\mathfrak{H})$. We easily see that (ρ, V) is a projective representation of $\mathfrak{H}$ belonging to c. Let V_i $(i=1,2)$ be equivalent $\mathcal{A}$-modules and (ρ_i, V_i) be the projective representations defined by the $\mathcal{A}$-modules V_i as above. Then there exists a character $\chi\in\widehat{\mathfrak{H}}$ and a K-isomorphism $\varphi: V_1\rightarrow V_2$ satisfying (26). We take sections T_i for ρ_i $(i=1,2)$ defined by the same base $\{e_H\}$ of $\mathcal{A}$. Then we have $\varphi\circ T_1(H)=(\chi(H)\, T_2(H))\circ\varphi$, whence $\tilde{\varphi}\circ\rho_1=\rho_2$ (Cf. § 1.2.) i.e. $\rho_1\sim\rho_2$. Thus we obtain the mapping

$$\mathfrak{M}_{\mathcal{A}}\rightarrow\mathfrak{P}_c\,. \tag{27}$$

We shall show that this mapping is injective. Suppose that (ρ_i, V_i) defined by the $\mathcal{A}$-modules V_i are equivalent. There exists a K-isomorphism $\varphi: V_1\rightarrow V_2$ such that $\tilde{\varphi}\circ\rho_1=\rho_2$. We take sections T_i for ρ_i $(i=1,2)$ which define the same cocycle $f\in c$. Then we have $\varphi\circ T_1(H)=\lambda_H\, T_2(H)\circ\varphi$ for some $\lambda_H\in K^*$. Hence

$$\varphi\circ T_1(P)\, T_1(Q)=f(P,Q)\,\varphi\circ T_1(PQ)=f(P,Q)\,\lambda_{PQ}T_2(PQ)\circ\varphi=\lambda_{PQ}\, T_2(P)\, T_2(Q)\circ\varphi\,.$$

Also we have

$$\varphi\circ T_1(P)\, T_1(Q)=\lambda_P\, T_2(P)\circ\varphi\circ T_1(Q)=\lambda_P\,\lambda_Q\, T_2(P)\, T_2(Q)\circ\varphi\,.$$

Therefore we have $\lambda_{PQ}=\lambda_P\,\lambda_Q$ whence the mapping

$$\chi: H\rightarrow\lambda_H \qquad (H\in\mathfrak{H})$$

is an element of $\widehat{\mathfrak{H}}=\mathrm{Hom}(\mathfrak{H}, K^*)$. Then

$$(\varphi\circ T_1(H))(v)=(\chi(H)\, T_2(H)\circ\varphi)(v)=(\chi(H)\, e_H)\varphi(v)$$

for all $H\in\mathfrak{H}$, $v\in V_1$. This implies $\varphi(a\, v)=\bar{\chi}(a)\,\varphi(v)$ for all $v\in V_1$, whence $V_1\sim V_2$.

Next, we shall show that the mapping (27) is surjective. Let (ρ, V) be any projective representation belonging to c, and T be a section for ρ which defines a cocycle $f\in c$. We take a base $\{e_H\}$ of $\mathcal{A}$ $(e_H\in\mathcal{A}_H^*)$ which defines the same cocycle f. Then we define a structure of $\mathcal{A}$-module on V as follows.

$$a\, v=\sum_{H\in\mathfrak{H}}\lambda_H\, T(H)\, v \qquad \text{for } v\in V,$$

where $a=\sum_{H\in\mathfrak{H}}\lambda_H\, e_H$ $(\lambda_H\in K)$. It is clear that this $\mathcal{A}$-module defines (ρ, V) by the above mentioned manner. This completes the proof of the bijectivity of the mapping (27).

It is easily seen that the equivalence classes of simple $\mathcal{A}$-modules and the equivalence classes of irreducible projective representations belonging to c correspond under the mapping (27). Moreover the semi-simplicity of algebra extensions impies the complete reducibility of projective representations.[25] Thus the problem to determine all projective representations of a finite group $\mathfrak{H}$ over a field K is reduced, in some sense, to the problem to determine all algebra extensions of $\mathfrak{H}$ over K and the actions of $\mathfrak{H}$ on these algebras. In § 6, we shall solve this problem for any abelian group $\mathfrak{H}$ and $\mathfrak{H}$-cyclic field.

5.3. Faithful representations and simple algebra extensions.

Let $\mathcal{A}$ be an algebra extension of a finite group $\mathfrak{H}$ over a field K, and c be the corresponding cohomology class in $\mathrm{H}^2(\mathfrak{H}, K^*)$. The left $\mathcal{A}$-module $\mathcal{A}$ defines a projective representation $(\rho_{\mathcal{A}}, \mathcal{A})$ where $\mathcal{A}$ is regarded as a representation space. This is nothing but the representation given in the proof of Proposition 1.2.

Let us consider the case that $\mathcal{A}$ is simple. Then we have a direct sum decomposition

$$\mathcal{A} = V_1 + V_2 + \cdots + V_n$$

where V_i are minimal left ideals. There exist $\mathcal{A}$-isomorphisms

$$\varphi_i : V_i \rightarrow V_1 \quad (i=1, 2, \cdots, n)$$

The simple $\mathcal{A}$-module V_1 defines an irreducible projective representation (ρ_1, V_1). Let $H \in \mathfrak{H}$ be in the kernel of ρ_1. Then $e_H v_1 = \lambda v_1$ for some $\lambda \in K$, $e_H \in \mathcal{A}_H^*$ and all $v_1 \in V_1$. Therefore we have

$$\varphi_i(e_H v_i) = e_H \varphi_i(v_i) = \lambda \varphi_i(v_i) = \varphi_i(\lambda v_i)$$

for all $v_i \in V_i$. Hence we have

$$e_H v_i = \lambda v_i \quad \text{for all } v_i \in V_i,$$

which implies $e_H v = \lambda v$ for all $v \in \mathcal{A}$. It follows that $H = I$, since $\rho_{\mathcal{A}}$ is faithful. Thus we have the following.

PROPOSITION 5.1. *Let $\mathcal{A}$ be an algebra extension of a finite group $\mathfrak{H}$ over a field K corresponding to $c \in \mathrm{H}^2(\mathfrak{H}, K^*)$. If $\mathcal{A}$ is simple, then all irreducible projective representations of $\mathfrak{H}$ over K belonging to c are equivalent and faithful.*

25) The direct sum of projective representations cannot be defined if the associated cohomology classes are different. Even if the cohomology classes coincide with each other, the direct sum is not necessarily unique.

The converse is, in general, not true (Cf. Remark after the Corollary to Proposition 5.2.). However we have

PROPOSITION 5.2. *Let $\mathcal{A}$ be an algebra extension of a finite group $\mathfrak{H}$ over an algebraically closed field K corresponding to $c \in H^2(\mathfrak{H}, K^*)$. If there exists a faithful irreducible projective representation belonging to c, then any $\mathcal{A}$-normal element of $\mathfrak{H}$ is not contained in the center of $\mathfrak{H}$ except the unit element.*

PROOF. Suppose that there exists an $\mathcal{A}$-normal element $N \neq I$ contained in the center of $\mathfrak{H}$. Then we have, for $f \in c$,

$$f(N, H)\, f(H, N)^{-1} = 1 \qquad \text{for all } H \in \mathfrak{H}.$$

Let (ρ, V) be any irreducible projective representation belonging to c, and T a section for ρ. We have

$$T(N)\, T(H) = T(H)\, T(N) \qquad \text{for all } H \in \mathfrak{H}.$$

By the usual Schur's lemma, it follows that $T(N)$ is in $K^* 1_V$, whence $\rho(N) = 1$. This means that ρ is not faithful. Proposition is thereby proved.

Proposition 4.1, Proposition 5.1 and Proposition 5.2 imply the following.

COROLLARY. *Let $\mathcal{A}$, c, K be as in Proposition 5.2 and $\mathfrak{H}$ be a finite abelian group. Then there exists a faithful irreducible projective representation belonging to c, if and only if $\mathcal{A}$ is central simple.*

REMARK. It is not essential in Corollary that $\mathfrak{H}$ is abelian. In fact, there exist central simple algebra extensions for suitable non-abelian groups (Iwahori-Matsumoto [15]). However such a finite group should have a square order, since a central simple algebra is of square rank. Therefore a finite simple group whose order is not square, has no central simple algebra extension but a faithful irreducible projective representation.

In § 6.2, we shall determine the finite abelian groups which have central simple algebra extensions.

§ 6. Algebra extensions of finite abelian groups.

6.1. The action of the character group.

In this section, we consider a finite abelian group $\mathfrak{H}$ exclusively. We assume that a field K is $\mathfrak{H}$-cyclic, or equivalently, $\mathfrak{H} \cong \hat{\mathfrak{H}} = \mathrm{Hom}(\mathfrak{H}, K^*)$ (Cf. § 3.2.). $\hat{\mathfrak{H}}$ acts on any algebra extension of $\mathfrak{H}$ over K, as stated in § 5.1.

THEOREM 6.1. *Let $\mathfrak{H}$ be a finite abelian group and K a $\mathfrak{H}$-cyclic field. Then any algebra extension $\mathcal{A}$ of $\mathfrak{H}$ over K is semi-simple; $\mathcal{A}$ is decomposed into the direct sum of all minimal ideals:*

$$\mathcal{A} = \mathcal{A}_1 + \mathcal{A}_2 + \cdots + \mathcal{A}_m\,.$$

The followings hold.

1) *The* $\mathcal{A}_i$ $(1 \leqq i \leqq m)$ *are mutually isomorphic simple algebras over* K.

2) *The center* L_i *of* $\mathcal{A}_i$ *is a Kummer extension*[26] *over* K *for each* i.

3) $\hat{\mathfrak{H}} = \mathrm{Hom}(\mathfrak{H}, K^*)$ *acts on* $\{\mathcal{A}_i\}_{1 \leqq i \leqq m}$ *transitively.*

4) $\mathfrak{g} = \{\chi \in \hat{\mathfrak{H}};\ \bar{\chi}(\mathcal{A}_i) = \mathcal{A}_i\}$ *is a subgroup of* $\hat{\mathfrak{H}}$ *independent of* i *such that* $[\hat{\mathfrak{H}} : \mathfrak{g}] = m$. $\mathfrak{g}$ *induces all automorphisms of* L_i *over* K.

5) $\mathfrak{g}_0 = \{\chi \in \mathfrak{g};\ \bar{\chi}(x) = x$ for all $x \in L_i\}$ *is a subgroup of* $\mathfrak{g}$ *independent of* i *such that* $[\mathfrak{g}_0 : 1] = [\mathcal{A}_i : L_i]$. $\mathfrak{g}_0$ *acts on the central simple algebra* $\mathcal{A}_i$ *over* L_i *faithfully for each* i.

PROOF. The characteristic of K does not divide the order of $\mathfrak{H}$, since K is $\mathfrak{H}$-cyclic. Therefore $\mathcal{A}$ is semi-simple by Theorem 4.1. We note that 3) implies 1) and the former part of 4) since $\mathfrak{H}$ is abelian. Furthermore 1), 2), 3), 4) imply 5). Thus it is sufficient to prove 2), 3) and the latter part of 4).

Let $\mathfrak{N}$ be the set of all $\mathcal{A}$-normal elements in $\mathfrak{H}$. Then $\mathfrak{N}$ is a subgroup of $\mathfrak{H}$ and the center of $\mathcal{A}$ is decomposed into the direct sum as follows (Cf. § 4.4.).

$$\mathcal{Z}(\mathcal{A}) = \sum_{N \in \mathfrak{N}}{}' \mathcal{A}_N$$

The center $\mathcal{Z}(\mathcal{A})$ has the structure of algebra extension of $\mathfrak{N}$ over K. Suppose that the theorem holds for commutative algebra extensions. Then $\mathcal{Z}(\mathcal{A})$ is decomposed into the direct sum of all minimal ideals as follows.

$$\mathcal{Z}(\mathcal{A}) = L_1 + L_2 + \cdots + L_m$$

where the L_i are isomorphic Kummer extensions over K. Moreover $\hat{\mathfrak{N}} = \mathrm{Hom}(\mathfrak{N}, K^*)$ acts on $\{L_i\}_{1 \leqq i \leqq m}$ transitively, and $\mathfrak{g} = \{\chi \in \hat{\mathfrak{N}};\ \chi(L_i) = L_i\}$, which is independent of i, induces all automorphisms of L_i over K. We take elements $e_i \in L_i$ such that $1 = e_1 + e_2 + \cdots + e_m$. Then the e_i are primitive orthogonal idempotents in the center of a semi-simple algebra $\mathcal{A}$. Therefore $\mathcal{A}$ is decomposed into the direct sum of ideals $\mathcal{A}_i = \mathcal{A}e_i$, which are simple. Clearly L_i is the center of $\mathcal{A}_i$ for each i, whence 2) holds. Any $\chi \in \hat{\mathfrak{N}}$ is extendible to $\chi' \in \hat{\mathfrak{H}}$, since K is $\mathfrak{H}$-cyclic. Therefore the action $\bar{\chi}$ $(\chi \in \hat{\mathfrak{N}})$ on $\mathcal{Z}(\mathcal{A})$ is the restriction of the action $\bar{\chi}'$ $(\chi' \in \hat{\mathfrak{H}})$ on $\mathcal{A}$ to $\mathcal{Z}(\mathcal{A})$. This implies 3) and the latter part of 4).

Thus we can assume that $\mathcal{A}$ is commutative. In this case, we use the induction on the number of generators of $\mathfrak{H}$. First, let $\mathfrak{H}$ be a cyclic group generated by S of order n, and $\mathcal{A}$ be an algebra extension of $\mathfrak{H}$ over K. We take an element $e_S \in \mathcal{A}_S^*$. Then e_S^n is in K^*; we denote by a this element. It follows that the assignment $X \to e_S$ induces an algebra isomorphism

26) This means that L_i is a Kummer extension of Ke_i where e_i is the unit element of $\mathcal{A}_i$.

(28) $$K[X]/(X^n-a)\cong\mathcal{A}$$

where $K[X]$ is the polynomial algebra of one variable X, and (X^n-a) is the ideal generated by X^n-a. For any $\chi\in\hat{\mathfrak{H}}$, we have an automorphism of $K[X]$ such that

$$f(X)\to f(\omega X)\qquad f(X)\in K[X],$$

where $\omega=\chi(S)$. Clearly this induces an automorphism of $K[X]/(X^n-a)$ which corresponds to $\bar{\chi}$ by the isomorphism (28). Now we identify $K[X]/(X^n-a)$ and $\mathcal{A}$ by (28). We fix a generator χ of $\hat{\mathfrak{H}}$, then $\omega=\chi(S)$ is a primitive n-th root of 1. Let d be the order of a modulo K^*.[27] Then $n=dm$ for an integer m. For some $b\in K^*$, we have $a=b^m$ and the factorization

$$X^n-a=\prod_{i=1}^{m}(X^d-\omega^{id}b),$$

whose factors are all irreducible in $K[X]$. Therefore we have a decomposition into a direct sum of ideals:

$$\mathcal{A}=K[X]/(X^n-a)=\sum_{i=1}^{m}{}^{\oplus}\mathcal{A}_i$$

where $\mathcal{A}_i$ is naturally isomorphic to $K[X]/(X^d-\omega^{id}b)\cong K(\sqrt[d]{b})$ which is a Kummer extension of K. If we take a polynomial $f_i(X)$ which represents the unit element of $\mathcal{A}_i$, we have

$$1\equiv\sum_{i=1}^{m}f_i(X)\qquad\text{mod. }(X^n-a),$$
$$f_i(X)\equiv\delta_{i,j}\qquad\text{mod. }(X^d-\omega^{jd}b).$$

By the automorphism $\bar{\chi}:f(X)\to f(\omega X)$,

$$f_i(X)\to f_i(\omega X)\equiv\delta_{i,j}\qquad\text{mod. }(X^d-\omega^{(j-1)d}b)$$
$$\equiv\delta_{i-1,j}\qquad\text{mod. }(X^d-\omega^{jd}b)^{28)}$$

Therefore we have $\bar{\chi}(\mathcal{A}_i)=\mathcal{A}_{i-1}$, whence $\hat{\mathfrak{H}}$ acts on $\{\mathcal{A}_i\}_{1\le i\le m}$ transitively, and $\bar{\chi}^m(\mathcal{A}_i)=\mathcal{A}_i$. Moreover the subgroup $\mathfrak{g}$ of $\hat{\mathfrak{H}}$ generated by χ^m acts on $\mathcal{A}_i$ faithfully. Then $\mathfrak{g}$ induces all automorphisms of $\mathcal{A}_i$ over K since $[\mathfrak{g}:1]=[\mathcal{A}_i:K]=d$. This completes the proof of the theorem for a cyclic group $\mathfrak{H}$. Moreover $\mathfrak{g}$ is isomorphic to the Galois group of $\mathcal{A}_i$ over K.

Next, let a finite abelian group $\mathfrak{H}$ be decomposed into a direct product of two subgroups as $\mathfrak{H}=\mathfrak{H}^{(1)}\times\mathfrak{H}^{(2)}$, and $\mathcal{A}$ be an algebra extension of $\mathfrak{H}$ over K which is commutative. Then we have two subalgebras

27) d is equal to the order of the cohomology class corresponding to $\mathcal{A}$.

28) Let i, j run modulo m.

$$\mathcal{A}^{(1)} = \sum_{H_1 \in \mathfrak{H}^{(1)}} \mathcal{A}_{H_1}, \quad \mathcal{A}^{(2)} = \sum_{H_2 \in \mathfrak{H}^{(2)}} \mathcal{A}_{H_2}$$

which are algebra extensions of $\mathfrak{H}^{(1)}$ and $\mathfrak{H}^{(2)}$ respectively. Furthermore we see that $\mathcal{A}$ is naturally isomorphic to the tensor product $\mathcal{A}^{(1)} \underset{K}{\otimes} \mathcal{A}^{(2)}$ since $\mathcal{A}$ is commutative; we identify these algebras. Now suppose that the theorem holds for $\mathcal{A}^{(1)}$ and $\mathcal{A}^{(2)}$. If $\chi \in \widehat{\mathfrak{H}}$ corresponds to $\chi^{(i)} \in \widehat{\mathfrak{H}^{(i)}}$ naturally $(i=1,2)$, we have $\bar{\chi} = \chi^{(1)} \otimes \chi^{(2)}$. Therefore the proof of the theorem has been reduced to the proof of the following proposition.[29]

PROPOSITION 6.1. *Let $\mathcal{A}$ be a commutative algebra over a field K and $\mathfrak{h}$ be a finite group acting on the algebra $\mathcal{A}$. If the following three conditions hold, we call the pair $(\mathcal{A}, \mathfrak{h})$ regular.*

1) *$\mathcal{A}$ is decomposed into the direct sum of all minimal ideals $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m$ where the $\mathcal{A}_i$ are mutually isomorphic Galois extensions over K.*

2) *$\mathfrak{h}$ acts on $\{\mathcal{A}_i\}_{1 \leq i \leq m}$ transitively.*

3) *The group $\mathfrak{g}_i = \{\chi \in \mathfrak{h};\ \bar{\chi}(\mathcal{A}_i) = \mathcal{A}_i\}$[30] is naturally isomorphic to the Galois group of $\mathcal{A}_i$ over K $(1 \leq i \leq m)$.*

Now let two pair $(\mathcal{A}^{(1)}, \mathfrak{g}^{(1)})$ and $(\mathcal{A}^{(2)}, \mathfrak{g}^{(2)})$ be regular. Then $\mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)}$ acts naturally on $\mathcal{A}^{(1)} \underset{K}{\otimes} \mathcal{A}^{(2)}$, and the pair $(\mathcal{A}^{(1)} \otimes \mathcal{A}^{(2)}, \mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)})$ is regular.

PROOF. Let $\mathcal{A}^{(1)} = \sum_i \mathcal{A}_i^{(1)}$ and $\mathcal{A}^{(2)} = \sum_j \mathcal{A}_j^{(2)}$ be the direct sum decompositions satisfying 1). Then we have the direct sum decomposition

$$\mathcal{A}^{(1)} \otimes \mathcal{A}^{(2)} = \sum_{i,j} \mathcal{A}_i^{(1)} \otimes \mathcal{A}_j^{(2)}$$

where $\mathcal{A}_i^{(1)} \otimes \mathcal{A}_j^{(2)}$ are ideals but not necessarily simple. $\mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)}$ acts naturally on $\{\mathcal{A}_i^{(1)} \otimes \mathcal{A}_j^{(2)}\}$ transitively, and the subgroup of $\mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)}$ consisting of all elements $\chi \in \mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)}$ such that $\bar{\chi}(\mathcal{A}_i^{(1)} \otimes \mathcal{A}_j^{(2)}) = \mathcal{A}_i^{(1)} \otimes \mathcal{A}_j^{(2)}$ is equal to $\mathfrak{g}_i^{(1)} \times \mathfrak{g}_j^{(2)}$. Therefore we can assume that $\mathcal{A}^{(1)}$ and $\mathcal{A}^{(2)}$ are Galois extensions over K. In this case, we have a decomposition into a direct sum of ideals:

$$\mathcal{A}^{(1)} \otimes \mathcal{A}^{(2)} = \sum_{i=1}^{m} L_i$$

where the L_i are isomorphic Galois extensions over K. Moreover $\mathfrak{h} = \mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)}$ acts on $\{L_i\}_{1 \leq i \leq m}$ transitively, and

$$\mathfrak{g}_i = \{\chi \in \mathfrak{g}^{(1)} \times \mathfrak{g}^{(2)};\ \bar{\chi}(L_i) = L_i\}$$

induces all automorphisms of L_i over K. Since $[\mathfrak{h} : \mathfrak{g}_i] = m$, we have $[\mathfrak{g}_i : 1] = [L_i : K]$. Therefore $\mathfrak{g}_i$ is naturally isomorphic to the Galois group of L_i over K. This completes

29) When $\mathfrak{h}$ is abelian, $\mathfrak{g}_i$ is independent of i.

30) $\bar{\chi}$ denotes the automorphism induced by χ.

the proof of Proposition 6.1.

Theorm 6.1. implies immediately the following (Cf. § 5.).

COROLLARY.[31] *Let $\mathfrak{H}$ be a finite abelian group and K a $\mathfrak{H}$-cyclic field. Then there exists only one equivalence class of irreducible projective representations of $\mathfrak{H}$ over K belonging to each cohomology class in* $H^2(\mathfrak{H}, K^*)$.

6.2. Characterization of the center.

Let $\mathfrak{H}, K, \mathcal{A}$ be as in Theorem 6.1 and φ be the corresponding anti-symmetric pairing in the sense of § 4.4. Then we have the center of $\mathcal{A}$ as follows.

$$\mathcal{Z}(\mathcal{A}) = \sum_{N \in \mathfrak{N}} \mathcal{A}_N$$

where $\mathfrak{N}$ is the annihilator of φ. We note that the group $\mathfrak{g}_0$ defined in Theorem 6.1 coincides with the group of all $\chi \in \hat{\mathfrak{H}}$ such that $\bar{\chi}$ fix any element of $\mathcal{Z}(\mathcal{A})$; we call $\mathfrak{g}_0$ the *fixed group* of $\mathcal{Z}(\mathcal{A})$. We easily see that

$$\begin{array}{cccc} \mathfrak{H} & 1 & \mathcal{A} & \mathcal{A}_i \\ | & | & | & | \\ \mathfrak{N} & \mathfrak{g}_0 & \mathcal{Z}(\mathcal{A}) & L_i \\ | & | & | & | \\ | & \mathfrak{g} & \sum_{i=1}^{m} Ke_i & Ke_i \\ | & | & | & \\ I & \hat{\mathfrak{H}} & K & \end{array}$$

$$\mathfrak{N} = \{H \in \mathfrak{H};\ \chi(H) = 1 \text{ for all } \chi \in \mathfrak{g}_0\},$$

whence we have naturally

$$\mathfrak{g}_0 \cong \widehat{\mathfrak{H}/\mathfrak{N}}, \qquad \dim_K \mathcal{Z}(\mathcal{A}) = [\mathfrak{N} : I] = [\hat{\mathfrak{H}} : \mathfrak{g}_0].$$

In the following we characterize the subgroup $\mathfrak{g}_0$ in $\hat{\mathfrak{H}}$, in other words, the subgroup $\mathfrak{N}$ in $\mathfrak{H}$.

We shall call a finite abelian group of "*symmetric type*" if it can be decomposed into a direct product of two isomorphic subgroups.

THEOREM 6.2. *Let $\mathfrak{H}$ be a finite abelian group and K a $\mathfrak{H}$-cyclic field. Then, for any algebra extension $\mathcal{A}$ of $\mathfrak{H}$ over K, the fixed group $\mathfrak{g}_0$ of the center $\mathcal{Z}(\mathcal{A})$ is of symmetric type. Conversely, for any subgroup $\mathfrak{g}_0$ of symmetric type of $\hat{\mathfrak{H}}$, there exists an algebra extension $\mathcal{A}$ of $\mathfrak{H}$ over K such that $\mathfrak{g}_0$ coincides with the fixed group of the center $\mathcal{Z}(\mathcal{A})$.*

PROOF. Let $\mathcal{A}, \varphi, \mathfrak{N}, \mathfrak{g}_0$ be as above, then $\mathfrak{g}_0 \cong \widehat{\mathfrak{H}/\mathfrak{N}}$. Therefore $\mathfrak{g}_0$ is of symmetric type if and only if $\mathfrak{H}/\mathfrak{N}$ is of symmetric type. Moreover φ induces a non-degenerate anti-symmetric pairing of $\mathfrak{H}/\mathfrak{N}$ into K^*, and conversely such a pairing is obtained by an anti-symmetric pairing of $\mathfrak{H}$ into K^* whose annihilator coincides with $\mathfrak{N}$. Thus Theorem is reduced to the following proposition, since anti-symmetric pairing of $\mathfrak{H}$ into K^* corresponds to some algebra extension of $\mathfrak{H}$ over K (Theorem

31) When $K = C$ (complex numbers), Frucht [4] proved this fact using the representation-groups. Also cf. [15].

2.2 and § 4.1.).

PROPOSITION 6.2. *Let $\mathfrak{H}$ be a finite abelian group and K a field. Then the following two conditions are equivalent.*

1) *There exists a non-degenerate anti-symmetric pairing of $\mathfrak{H}$ into K^*.*

2) *$\mathfrak{H}$ is of symmetric type and K is $\mathfrak{H}$-cyclic.*

PROOF. 1)$\Rightarrow$2). Let φ be a non-degenerate anti-smmetric pairing of $\mathfrak{H}$ into K^*. For $P\in\mathfrak{H}$, we set

$$\varphi_P(X)=\varphi(P, X) \qquad (X\in\mathfrak{H}).$$

Then we have an injective homomorphism of $\mathfrak{H}$ into $\hat{\mathfrak{H}}$ defined by $P\to\varphi_P$. However $[\mathfrak{H}:I]\geq[\hat{\mathfrak{H}}:1]$, therefore this homomorphism is bijective and K is $\mathfrak{H}$-cyclic.

Now we take an element S in $\mathfrak{H}$ whose order n is the maximum in $\mathfrak{H}$. Then the order of φ_S is also equal to n. Since the orders of all elements in $\mathfrak{H}$ divide n, there exists an element T in $\mathfrak{H}$ such that its order is equal to n and $\varphi_S(T)=\omega$ is a primitive n-th root of 1. Namely we have

$$\begin{cases} \varphi(S, S)=\varphi(T, T)=1\,, \\ \varphi(S, T)=\omega\,,\ \varphi(T, S)=\omega^{-1}\,. \end{cases} \tag{29}$$

If $S^i=T^j$ for some i and j, we have

$$\omega^i=\varphi(S, T)^i=\varphi(S^i, T)=\varphi(T^j, T)=\varphi(T, T)^j=1\,.$$

Therefore i is divisible by n, whence $S^i=T^j=I$. This shows that the subgroup $\mathfrak{H}_1$ of $\mathfrak{H}$ generated by S and T is decomposed into a direct product of two cyclic subgroups of the same order n. Hence $\mathfrak{H}_1$ is of symmetric type.

Next, we take another subgroup of $\mathfrak{H}$ defined by

$$\mathfrak{H}_2=\{X\in\mathfrak{H}\,;\ \varphi(H, X)=1 \text{ for all } H\in\mathfrak{H}_1\}\,.$$

Let S^iT^j be in $\mathfrak{H}_1\cap\mathfrak{H}_2$. Then we have

$$\varphi(S, S^iT^j)=\varphi(T, S^iT^j)=1\,. \tag{30}$$

From (29) and (30), it follows that $\omega^j=\omega^{-i}=1$. Therefore i and j are divisible by n whence $S^iT^j=I$. This yields $\mathfrak{H}_1\cap\mathfrak{H}_2=\{I\}$. Furthermore $\mathfrak{H}_2$ is the annihilator of the subgroup of $\hat{\mathfrak{H}}$ corresponding to $\mathfrak{H}_1$ by the isomorphism $H\to\varphi_H$. Therefore we have $[\mathfrak{H}_2:I]=[\mathfrak{H}:\mathfrak{H}_1]$. Thus we obtain the direct product decomposition

$$\mathfrak{H}=\mathfrak{H}_1\times\mathfrak{H}_2\,.$$

Moreover φ induces a non-degenerate anti-symmetric pairing φ_2 of $\mathfrak{H}_2$ into K^*, since $\varphi(H_1, H_2)=1$ for all $H_i\in\mathfrak{H}_i$ $(i=1, 2)$. Therefore the inductive argument deduces that

$\mathfrak{H}$ is of symmetric type.

2)$\Rightarrow$1). Let $\mathfrak{H}_1$ and $\mathfrak{H}_2$ be finite abelian groups of symmetric type such that there exists a non-degenerate anti-symmetric pairing φ_i of $\mathfrak{H}_i$ into K^* for each i. If we define an anti-symmetric pairing φ of the direct product $\mathfrak{H}_1 \times \mathfrak{H}_2$ into K^* by

$$\varphi(P_1 P_2, Q_1 Q_2) = \varphi_1(P_1, Q_1)\, \varphi_2(P_2, Q_2) \qquad (P_i, Q_i \in \mathfrak{H}_i),$$

it is easily seen that φ is non-degenerate. On the other hand any finite abelian group of symmetric type is decomposed into a direct product of subgroups $\mathfrak{H}_i$ $(1 \leq i \leq m)$ such that each $\mathfrak{H}_i$ is a direct product of two isomorphic cyclic subgroups. Therefore it is sufficient to prove 2)$\Rightarrow$1) for a group $\mathfrak{H}$ which is a direct product of two isomorphic cyclic subgroups generated by S and T respectively.

Let n be the order of S and T. We can define a pairing φ of $\mathfrak{H}$ into K^* by (29), where ω is a primitive n-th root of 1. Clearly φ is anti-symmetric. If $\varphi(X, S^i T^j) = 1$ for all $X \in \mathfrak{H}$, we have (30). Therefore, by (29) and (30), we have $\omega^j = \omega^{-i} = 1$ as before, whence $S^i T^j = I$. Namely we see that φ is non-degenerate. This completes the proof of 2)$\Rightarrow$1). Proposition 6.2 is thereby proved.

THEOREM 6.3.[32] *Let $\mathfrak{H}$ be a finite abelian group and K a field. Then there exists a central simple algebra extension of $\mathfrak{H}$ over K if and only if $\mathfrak{H}$ is of symmetric type and K is $\mathfrak{H}$-cyclic.*

PROOF. Any anti-symmetric pairing of $\mathfrak{H}$ into K^* corresponds to an algebra extension of $\mathfrak{H}$ over K. Therefore Theorem follows from Proposition 4.1 and the above Proposition 6.2.

Proposition 5.1, Corollary to Proposition 5.2 and the above Theorem 6.3 imply immediately the following.

COROLLARY. *Let $\mathfrak{H}$ be a finite abelian group and K a $\mathfrak{H}$-cyclic field. Then there exists a faithful irreducible projective representation of $\mathfrak{H}$ over K, if $\mathfrak{H}$ is of symmetric type. Moreover, the converse holds if K is algebraically closed.*

§ 7. Applications and examples of algebra extensions.

7.1. Isotypical components of a module.

In this section, we consider a canonical decomposition of any faithful linear representation of a finite abelian group as a preliminary for § 7.2 and § 7.4.

Let $\mathfrak{A}$ be a finite abelian group and V a vector space over an $\mathfrak{A}$-cyclic field (Cf. § 3.2.); we note that the characteristic of K does not divide the order of $\mathfrak{A}$. Assume that $\mathfrak{A}$ acts on V faithfully; we denote by $v \rightarrow {}^A v$ the action of $A (v \in V, A \in \mathfrak{A})$.

32) This was suggested by N. Iwahori, and he proved "if" part by another method.

For each $\chi\in\hat{\mathfrak{A}}=\mathrm{Hom}(\mathfrak{A}, K^*)$, we take an $\mathfrak{A}$-invariant subspace of V defined by

$$V_\chi=\{v\in V;\ {}^A v=\chi(A)v \text{ for all } A\in\mathfrak{A}\}.$$

Now we define a sum[33)]

$$S(\chi, v)=(1/|\mathfrak{A}|)\sum_{A\in\mathfrak{A}}\chi(A^{-1})\,{}^A v$$

where $|\mathfrak{A}|$ denotes the order of $\mathfrak{A}$.

PROPOSITION 7.1. *Let* $\mathfrak{A}$, K, V, V_χ *and* $S(\chi, v)$ $(\chi\in\hat{\mathfrak{A}}, v\in V)$ *be as above. Then we have*

1) V *is decomposed into the direct sum of all* V_χ $(\chi\in\hat{\mathfrak{A}})$.

2) *The mapping* $v\rightarrow S(\chi, v)$ *coincides with the projection of* V *onto* V_χ *w.r.t. the above direct sum decomposition.*

PROOF. We easily see that

$$S(\chi, {}^A v)={}^A S(\chi, v)=\chi(A)\,S(\chi, v)$$

since $\mathfrak{A}$ is abelian and χ is a homomorphism. Therefore the mapping $v\rightarrow S(\chi, v)$ is $\mathfrak{A}$-linear and the image is contained in V_χ for each $\chi\in\hat{\mathfrak{A}}$. Let v be any element of V_χ $(\chi\in\hat{\mathfrak{A}})$. Then we have

$$S(\chi', v)=(1/|\mathfrak{A}|)\sum_{A\in\mathfrak{A}}\chi'(A^{-1})\,{}^A v=(1/|\mathfrak{A}|)\sum_{A\in\mathfrak{A}}\chi'(A^{-1})\,\chi(A)\,v$$
$$=\begin{cases} v & \text{if } \chi'=\chi\,, \\ 0 & \text{if } \chi'\neq\chi \end{cases}$$

for $\chi'\in\hat{\mathfrak{A}}$. From this, it follows that V is decomposed into the direct sum of all V_χ $(\chi\in\hat{\mathfrak{A}})$. In fact, if

$$\sum_{\chi\in\hat{\mathfrak{A}}} v_\chi=0 \qquad (v_\chi\in V_\chi)\,,$$

then we have

$$0=S(\chi', \sum_\chi v_\chi)=v_{\chi'} \quad \text{for all } \chi'\in\hat{\mathfrak{A}}\,.$$

For any $v\in V$, we have

$$\sum_{\chi\in\hat{\mathfrak{A}}} S(\chi, v)=(1/|\mathfrak{A}|)\sum_{\chi\in\hat{\mathfrak{A}}}\ \sum_{A\in\mathfrak{A}}\chi(A^{-1})\,{}^A v$$
$$=(1/|\mathfrak{A}|)\sum_{A\in\mathfrak{A}}\Big(\sum_{\chi\in\hat{\mathfrak{A}}}\chi(A)^{-1}\Big)\,{}^A v=v\,.$$

This completes the proof.

We note that V is a semi-simple $\mathfrak{A}$-module and V_χ is an isotypical component

33) This a generalization of the classical Gauss's sum, when K is not assumed to be $\mathfrak{A}$-cyclic.

of $\mathfrak{A}$-module V for each $\chi\in\hat{\mathfrak{A}}$. In addition, when K is not assumed to be $\mathfrak{A}$-cyclic, $\sum_{\chi\in\hat{\mathfrak{A}}} V_\chi$ is not necessarily equal to V.

7.2. Group algebras of central group extensions.

Let $\mathfrak{H}$ be a finite group. There exist generally several non-isomorphic representation-groups of $\mathfrak{H}$. For example, let $\mathfrak{H}$ be a non-cyclic group of order 4 (which is isomorphic to $Z_2\times Z_2$). Then the multiplier $\mathfrak{M}(\mathfrak{H})=\mathrm{H}^2(\mathfrak{H}, C^*)$ is of order 2. Therefore there exist four non-equivalent representation-groups of $\mathfrak{H}$ which are of order 8 (Corollary 2 to Theorem 3.1). Three of them are isomorphic to the dihedral group $\mathfrak{D}_4$, and the other is isomorphic to the quaternion group. These two groups are of course not isomorphic. However it is well known that the group algebras of these two groups are isomorphic. We can prove such a fact for any finite group $\mathfrak{H}$ (Corollary to Theorem 7.1). More generally, we have the following.

THEOREM 7.1. *Let $\mathfrak{H}$ be a finite group, $\mathfrak{A}$ a finite abelian group and $(\mathfrak{G}, \pi)$ a central group extension of $\mathfrak{H}$ by $\mathfrak{A}$. Then the group algebra $K[\mathfrak{G}]$ of $\mathfrak{G}$ over an $\mathfrak{A}$-cyclic field K is decomposed into a direct sum of ideals as follows.*

$$K[\mathfrak{G}]=\sum_{\chi\in\hat{\mathfrak{A}}} \mathcal{A}_\chi$$

where $\mathcal{A}_\chi$ is isomorphic to the algebra extension of $\mathfrak{H}$ corresponding to $c_\chi\in \mathrm{H}^2(\mathfrak{H}, K^*)$ which is the image of χ by the transgression mapping τ (Cf. § 1.3 and § 1.4.), *for each $\chi\in\hat{\mathfrak{A}}=\mathrm{Hom}(\mathfrak{A}, K^*)$.*

PROOF. $\mathfrak{A}$ acts faithfully on $V=K[\mathfrak{G}]$, which is regarded as a vector space over K, by the left multiplication in the group algebra. Therefore, by Proposition 7.1, we have the direct sum decomposition

$$K[\mathfrak{G}]=\sum_{\chi\in\hat{\mathfrak{A}}} \mathcal{A}_\chi$$

where $\mathcal{A}_\chi=\{v\in K[\mathfrak{G}]\,;\ Av=\chi(A)v \text{ for all } A\in\mathfrak{A}\}$. The $\mathcal{A}_\chi$ are not only $\mathfrak{A}$-invariant but also ideals in $K[\mathfrak{G}]$. In fact, for any $A\in\mathfrak{A}$, $G\in\mathfrak{G}$ and $v\in\mathcal{A}_\chi$, we have

$$A(Gv)=G(Av)=\chi(A)(Gv)$$
$$A(vG)=(Av)G=\chi(A)(vG)\,.$$

Therefore $G\mathcal{A}_\chi$ and $\mathcal{A}_\chi G$ are contained in $\mathcal{A}_\chi$ for any $G\in\mathfrak{G}$, whence $\mathcal{A}_\chi$ is an ideal of $K[\mathfrak{G}]$ for each $\chi\in\hat{\mathfrak{A}}$.

Now we shall introduce structures of algebra extension into the algebras $\mathcal{A}_\chi$. Let u be a section of the group extension $(\mathfrak{G}, \pi)$ where $u(I)=I$, and we set $A(P, Q)=u(P)\,u(Q)\,u(PQ)^{-1}\in\mathfrak{A}$ $(P, Q\in\mathfrak{H})$. Using the notation in § 7.1, we define

$$e_{\chi, H}=S(\chi, u(H)) .$$

Then we have

$$(31)\qquad e_{\chi, H}=(1/|\mathfrak{A}|) \sum_{A\in\mathfrak{A}}' \chi(A^{-1})\, A\, u(H)=e_{\chi, I}\, u(H)$$

and easily see that the $e_{\chi, H}(H\in\mathfrak{H})$ are linearly independent over K for a fixed χ, whence $\dim \mathcal{A}_\chi \geq [\mathfrak{H}:I]$. However we have $[\mathfrak{G}:I]=\dim K[\mathfrak{G}]=\sum_{\chi\in\hat{\mathfrak{A}}}' \dim \mathcal{A}_\chi$. These show that $\dim \mathcal{A}_\chi=[\mathfrak{H}:I]$ for each $\chi\in\hat{\mathfrak{A}}$. Therefore the family $\{e_{\chi, H}\}_{H\in\mathfrak{H}}$ is a base of $\mathcal{A}_\chi$ for each χ. If we set $\mathcal{A}_{\chi, H}=Ke_{\chi, H}$, we have the direct sum decomposition

$$\mathcal{A}_\chi=\sum_{H\in\mathfrak{H}}' \mathcal{A}_{\chi, H}$$

where $\dim \mathcal{A}_{\chi, H}=1$ and $\mathcal{A}_{\chi, P}\mathcal{A}_{\chi, Q}=\mathcal{A}_{\chi, PQ}$. More explicitly, $e_{\chi, I}$ is the unit element of $\mathcal{A}_\chi$, since for any $v\in\mathcal{A}_\chi$ we have

$$v\, e_{\chi, I}=e_{\chi, I}\, v=(1/|\mathfrak{A}|) \sum_{A\in\mathfrak{A}}' \chi(A^{-1})A\, v=(1/|\mathfrak{A}|) \sum_{A\in\mathfrak{A}}' \chi(A^{-1})\, \chi(A)v=v .$$

Moreover we have, from (31),

$$\begin{aligned} e_{\chi, P}\, e_{\chi, Q}&=e_{\chi, I}\, u(P)\, e_{\chi, I}\, u(Q)=e_{\chi, I}\, u(P)\, u(Q)=e_{\chi, I}\, A(P, Q)\, u(PQ)\\ &=A(P, Q)\, e_{\chi, I}\, u(PQ)=\chi(A(P, Q))\, e_{\chi, I}\, u(PQ)=\chi(A(P, Q))\, e_{\chi, PQ} \end{aligned}$$

Thus A_χ is isomorphic to the algebra extension of $\mathfrak{H}$ over K corresponding to the cocycle $\{\chi(A(P, Q))\}$. This completes the proof.

COROLLARY 1. *Let $\mathfrak{H}$ be a finite group, $\mathfrak{A}$ a finite abelian group and K an $\mathfrak{A}$-cyclic field. Then the structure of group algebra of a central group extension of $\mathfrak{H}$ by $\mathfrak{A}$ over K depends only on $\mathfrak{H}$, K, the image of the transgression mapping $\tau: \hat{\mathfrak{A}}\to H^2(\mathfrak{H}, K^*)$, and the order of $\mathfrak{A}$.*

For the sake of simplicity, we assume that K is an algebraically closed field of characteristic 0. Then we have immediately the following.

COROLLARY 2. *Let K be an algebraically closed field of characteristic* 0. *Let $\mathfrak{H}$ be a finite group and $\mathfrak{G}$ any representation-group of $\mathfrak{H}$. Then the group algebra of $\mathfrak{G}$ over K is isomorphic to the direct sum of all non-isomorphic algebra extensions of $\mathfrak{H}$ over K.*

7.3. Total matric algebras and others.

In § 6, we studied the structures of algebra extension of a given finite abelian group and a condition for the existence of central simple algebra extensions. In the present and next sections, we shall start from simple algebras without any structure of algebra extension, and try to introduce such a structure into these algebras. First, we have the following.

PROPOSITION 7.2. *Let K be a field and K_n the total matric algebra of degree n over K. K_n is isomorphic to an algebra extension of a finite abelian group over K if and only if K contains a primitive p-th root of 1 for every prime divisor p of n.*

PROOF. Let K_n be isomorphic to an algebra extension of a finite abelian group $\mathfrak{H}$ over K. By Theorem 6.3, K is $\mathfrak{H}$-cyclic. Since the order of $\mathfrak{H}$ is equal to n^2, K contains a primitive p-th root of 1 for every prime divisor p of n.

Conversely, suppose that K contains a primitive p-th root ω_p of 1 for every prime divisor p of n. We denote by $\mathfrak{H}^{(p)}$ the direct product group of two cyclic groups of order p generated by S and T respectively. We define a pairing f of $\mathfrak{H}^{(p)}$ into K^* by the following relations.

$$f(S, S)=f(T, T)=1\,,$$
$$f(S, T)=\omega_p\,, \quad f(T, S)=1\,.$$

Since f is a 2-cocycle of $\mathfrak{H}^{(p)}$ in K^*, we have an algebra extension $\mathcal{A}^{(p)}$ of $\mathfrak{H}^{(p)}$ over K corresponding to f. f determines an anti-symmetric pairing φ satisfying (29) in the proof of Proposition 6.2, where $\omega=\omega_p$. Therefore φ is non-degenerate which implies $\mathcal{A}^{(p)}$ is central simple over K. We take a base $\{e_{S^i T^j}\}_{0\leqq i,\, j<p}$ corresponding to f. Then we see $e_S^p=1$, since $f(S, S)=1$. Therefore we have

$$(1-e_S)(1+e_S+e_S^2+\cdots+e_S^{p-1})=0\,,$$

whence $1-e_S$ is a zero-divisor in $\mathcal{A}^{(p)}$. Since $\mathcal{A}^{(p)}$ is central simple of rank p^2 where p is a prime number, it follows that $\mathcal{A}^{(p)}$ is isomorphic to the total matric algebra K_p of degree p over K.

Now we decompose n into the product of prime divisors $p_1, p_2, \cdots, p_s$ and consider the algebra extensions $\mathcal{A}^{(p_i)}$ over K as above. Then we have an algebra extension $\mathcal{A}$ of $\mathfrak{H}=\mathfrak{H}^{(p_1)}\times\mathfrak{H}^{(p_2)}\times\cdots\times\mathfrak{H}^{(p_s)}$ over K defined by

$$\mathcal{A}=\mathcal{A}^{(p_1)}\otimes\mathcal{A}^{(p_2)}\otimes\cdots\otimes\mathcal{A}^{(p_s)}$$

which is isomorphic to $K_{p_1}\otimes K_{p_2}\otimes\cdots\otimes K_{p_s}\cong K_n$.

This completes the proof.

Next, we consider semi-simple algebras of some type (Cf. Theorem 6.1.). Let $\mathcal{S}$ be an algebra extension of a finite group $\mathfrak{H}$ over K and $\mathcal{A}$ be a direct sum of ideals $\mathcal{A}_i$ $(1\leqq i\leqq m)$ which are all isomorphic to $\mathcal{S}$. Suppose that we can take a finite abelian group $\mathfrak{M}$ of order m such that K is $\mathfrak{M}$-cyclic. Then we have

$$\mathcal{A}\cong\mathcal{S}\underset{K}{\otimes}\mathcal{T}$$

where $\mathcal{T}$ is the group algebra of $\mathfrak{M}$ over K. Moreover the algebra $\mathcal{S}\underset{K}{\otimes}\mathcal{T}$ has naturally a structure of an algebra extension of $\mathfrak{H}\times\mathfrak{M}$ over K. For the sake of simplicity, we assume that K is algebraically closed of characteristic 0. Then we have

PROPOSITION 7.3. *Let $\mathcal{A}$ be an algebra of finite rank over an algebraically closed field K of characteristic 0. Then $\mathcal{A}$ is isomorphic to an algebra extension of a finite abelian group if and only if $\mathcal{A}$ is decomposed into a direct sum of ideals which are all isomorphic to the same total matric algebra.*

REMARK. Proposition 7.3 characterize the structure of algebra extensions of abelian groups. On the contrary, for non-abelian groups, simple components of algebra extensions are not necessarily isomorphic. For example, $\mathfrak{S}_4$ (the symmetric group) has two algebra extensions over the above field. The one is isomorphic to $K+K+K_2+K_3+K_3$ (group algebra) and the other is isomorphic to $K_2+K_2+K_4$.

7.4. The canonical structure of algebra extensions on simple algebras.

In this section, we consider a simple algebra over a field K with an abelian group of automorphisms. For a typical example, we have any Kummer extension of K; we can introduce into this extension a structure of algebra extension of the character group of the Galois group canonically. More generally we have

THEOREM 7.2. *Let $\mathcal{A}$ be an algebra over a field K and $\mathfrak{A}$ be a finite abelian group of automorphisms of $\mathcal{A}$ over K such that any element of $\mathcal{A}$ fixed by $\mathfrak{A}$ is contained in K. Furthermore we assume that one of the following two conditions is satisfied.*

1) *$\mathcal{A}$ is a central simple algebra.*

2) *$\mathcal{A}$ is a Kummer extension of K. i.e. $\mathcal{A}$ is a commutative field and K is $\mathfrak{A}$-cyclic.*

Then the family of submodules $\mathcal{A}_\chi=\{a\in\mathcal{A};\ {}^\sigma a=\chi(\sigma)\ \ a$ for all $\sigma\in\mathfrak{A}\}$ $(\chi\in\hat{\mathfrak{A}})$ is a structure of algebra extension of $\hat{\mathfrak{A}}=\mathrm{Hom}(\mathfrak{A}, K^*)$ on $\mathcal{A}$.

PROOF. When K is $\mathfrak{A}$-cyclic, by Proposition 7.1, we have the direct sum decomposition $\mathcal{A}=\sum_{\chi\in\hat{\mathfrak{A}}}\mathcal{A}_\chi$. Since $\mathfrak{A}$ is a group of algebra automorphisms, it is easily seen that $\mathcal{A}_\chi\mathcal{A}_{\chi'}\subset\mathcal{A}_{\chi\chi'}$. Therefore it is sufficient to prove that K is $\mathfrak{A}$-cyclic, that $\mathcal{A}_\chi^*$ contains an regular element of $\mathcal{A}$ in the case 1), and that $\dim_K\mathcal{A}_\chi=1$ in the both cases.

Case 1). Since $\mathcal{A}$ is central simple over K, there exist regular elements e_σ in $\mathcal{A}$ $(\sigma\in\mathfrak{A})$ such that

$${}^\sigma a=e_\sigma\, a\, e_\sigma^{-1} \quad \text{for all } a\in\mathcal{A}\,.$$

We note that any element e'_σ satisfying the above property is contained in $K^* e_\sigma$ for each $\sigma \in \mathfrak{A}$. In fact, if $e_\sigma a e_\sigma^{-1} = e'_\sigma a e'^{-1}_\sigma$ for all $a \in \mathcal{A}$, we have $a e_\sigma^{-1} e'_\sigma = e_\sigma^{-1} e'_\sigma a$ for all $a \in \mathcal{A}$. It follows that $e_\sigma^{-1} e'_\sigma \in K^*$ since $\mathcal{A}$ is central over K.

We see that

$$f(\sigma, \tau) = e_\sigma e_\tau e_{\sigma\tau}^{-1}$$

is contained in K^*. Moreover we easily see that f is a 2-cocycle of $\mathfrak{A}$ in K^*. (Note that $e_\sigma e_\tau e_{\sigma\tau}^{-1} = e_{\sigma\tau}^{-1} e_\sigma e_\tau$.) Thus we obtain an anti-symmetric pairing φ of $\mathfrak{A}$ into K^* defined by

$$\varphi(\sigma, \tau) = f(\sigma, \tau) f(\tau, \sigma)^{-1} = e_\sigma e_\tau e_\sigma^{-1} e_\tau^{-1}$$

$(\sigma, \tau \in \mathfrak{A})$. If we set $\psi_\tau(\sigma) = \varphi(\sigma, \tau)$, the mapping $\tau \to \psi_\tau$ is an injective homomorphism of $\mathfrak{A}$ into $\hat{\mathfrak{A}}$. In fact, suppose that $\psi_\tau(\sigma) = 1$ for all $\sigma \in \mathfrak{A}$. Then we have $e_\sigma e_\tau e_\sigma^{-1} e_\tau^{-1} = 1$ for all $\sigma \in \mathfrak{A}$, that is, ${}^\sigma e_\tau = e_\tau$ for all $\sigma \in \mathfrak{A}$. It follows that $e_\tau \in K^*$ by the assumption on $\mathcal{A}$, whence τ is the identity automorphism. Therefore the mapping $\tau \to \psi_\tau$ is injective, and thereby bijective. This implies that K is $\mathfrak{A}$-cyclic.

Now for any $\chi \in \hat{\mathfrak{A}}$, we take $\tau \in \mathfrak{A}$ such that $\psi_\tau = \chi$. Then we have

$${}^\sigma e_\tau = e_\sigma e_\tau e_\sigma^{-1} = \chi(\sigma) e_\tau \quad \text{for all } \sigma \in \mathfrak{A},$$

whence $e_\chi \in \mathcal{A}_\chi$. Namely $\mathcal{A}_\chi$ contains a regular element, and $\dim_K \mathcal{A}_\chi \geqq 1$. Let a be any element of $\mathcal{A}_\chi$. Then we have

$${}^\sigma a = \chi(\sigma) a = {}^\sigma e_\tau e_\tau^{-1} a \quad \text{for all } \sigma \in \mathfrak{A}.$$

Hence we have ${}^\sigma(e_\tau^{-1} a) = e_\tau^{-1} a$ for all $\sigma \in \mathfrak{A}$. It follows that $e_\tau^{-1} a \in K$ by the assumption. Therefore we have $\dim_K \mathcal{A}_\chi = 1$.

Case 2). Clearly we have $\dim_K \mathcal{A}_\chi \leqq 1$ by the similar way as above, since any non-zero element of $\mathcal{A}$ is regular. Hence it follows that $\dim_K \mathcal{A}_\chi = 1$ for every $\chi \in \hat{\mathfrak{A}}$.[34] This completes the proof.

7.5. A generalization of the Clifford algebra.

In this section, we define a special kind of an algebra extension which is a generalization of the usual Clifford algebra.[35]

Let n be a positive integer $\geqq 2$ and K a field containing a primitive n-th root ω of 1. Let $\mathfrak{H}$ be an abelian group decomposed into a direct product of m cyclic subgroups of the same order n which are generated by S_i $(i = 1, 2, \cdots, m)$ re-

34) The existence of non-zero elements in $\mathcal{A}_\chi$ is closely related to the fact that $H^1(\mathfrak{A}, \mathcal{A})$ is trivial.

35) Cf. C. Chevalley [Theory of Lie groups I. (1946)] and Y. Kawada - N. Iwahori [On the structure and representations of Clifford algebras, J. Math. Soc. Japan 2 (1950), 34-43.].

spectively:

$$\mathfrak{H}=(S_1)\times(S_2)\times\cdots\times(S_m).$$

We define a pairing f of $\mathfrak{H}$ into K^* as follows.

$$f(S_i, S_j)=\begin{cases} \omega & \text{if } i\leqq j, \\ 1 & \text{if } i>j. \end{cases}$$

Since f is a 2-cocycle of $\mathfrak{H}$ in K^*, f determines an algebra extension $\mathcal{A}_m^{(n)}$ of $\mathfrak{H}$ over K.

PROPOSITION 7.4. *If m is even, the algebra $\mathcal{A}_m^{(n)}$ is central simple. If m is odd, the center of $\mathcal{A}_m^{(n)}$ is of dimension n.*

PROOF. Let φ be the corresponding anti-symmetric pairing. Namely we define φ by $\varphi(P, Q)=f(P, Q)f(Q, P)^{-1}$ $(P, Q\in\mathfrak{H})$. Then we have

$$\varphi(S_i, S_j)=\begin{cases} \omega & (i<j) \\ 1 & (i=j) \\ \omega^{-1} & (i>j). \end{cases}$$

Let us determine the annihilator $\mathfrak{N}$ of φ and the center of $\mathcal{A}_m^{(n)}$ (Cf. § 4.4.). Let $H=\prod_{i=1}^{m} S_i^{\nu_i}$ be any element of $\mathfrak{H}$. Then H is contained in $\mathfrak{N}$ if and only if

$$\varphi(\prod_{i=1}^{m} S_i^{\nu_i}, S_j)=1 \quad \text{for } j=1, 2,\cdots, m.$$

Hence H is contained in $\mathfrak{N}$ if and only if

$$\prod_{i<j}\omega^{\nu_i}=\prod_{k>j}\omega^{\nu_k} \quad \text{for } j=1, 2,\cdots, m.$$

Since ω is a primitive n-th root of 1, this condition is equivalent to the following.

$$\sum_{i<j}\nu_i\equiv\sum_{k>j}\nu_k \pmod{n} \quad \text{for } j=1, 2,\cdots, m. \tag{32}$$

This implies that

$$\left.\begin{array}{ll} \nu_i+\nu_{i+1}\equiv 0 & (i=1, 2,\cdots, m-1) \\ \nu_1+\nu_2+\cdots+\nu_{m-1}\equiv 0 & \end{array}\right\} \pmod{n}.$$

If m is even, we have all $\nu_i\equiv 0 \pmod{n}$. This shows that $\mathfrak{N}=\{I\}$, whence $\mathcal{A}_m^{(n)}$ is central simple. If m is odd, we have

$$\nu_1\equiv\nu_3\equiv\cdots\equiv\nu_m\equiv-\nu_2\equiv-\nu_4\equiv\cdots\equiv-\nu_{m-1} \pmod{n}$$

which implies (32). This shows that $\mathfrak{N}$ is generated by the element $N=\prod_{i:\text{ odd}} S_i \prod_{j:\text{ even}} S_j^{-1}$, whose order is equal to n. This completes the proof of Proposition 7.4.

REMARK. When m is odd, in detail, the following two cases occur (Cf.

Theorem 6.1.).

Case 1). $n\equiv 0$ (mod. 2), $m\equiv 1$ (mod. 4) and K contains no primitive $2n$-th root of 1. In this case, $\mathcal{A}_m^{(n)}$ is decomposed into the direct sum of $n/2$ isomorphic simple ideals whose centers are isomorphic to the quadratic field $K(\sqrt{\omega})$.

Case 2). Otherwise. $\mathcal{A}_m^{(n)}$ is decomposed into the direct sum of n isomorphic central simple ideals.

Now we take a base $\{e_H\}_{H\in\mathfrak{H}}$ of $\mathcal{A}_m^{(n)}$ which determines the above cocycle f and let e_i denote e_{S_i} for each i. In particular, if $n=2$, then we have

$$e_i^2=-1\,,\qquad e_ie_j+e_je_i=0\,,$$

and $\{e_{i_1}\cdots e_{i_k}\}$ $(1\leqq i_1<\cdots<i_k\leqq m)$ with 1 constitute a base of $\mathcal{A}_m^{(2)}$. Namely $\mathcal{A}_m^{(2)}$ is nothing but the Clifford algebra. In general, the algebras $\mathcal{A}_m^{(n)}$ may be defined in such a form. Let V be an m-dimensional vector space over a field K. Suppose that an algebra $\mathcal{A}$ is generated by V as algebra over K and satisfies the following two conditions. (ω denotes a primitive n-th root of 1.)

1) There exists a base $\{e_i\}_{1\leqq i\leqq m}$ of V such that

$$\begin{aligned}&e_je_i=\omega e_ie_j \qquad (i>j)\\&e_i^n\in K^*1\end{aligned}$$

2) $\dim_K\mathcal{A}=n^m$.

Clearly $\mathcal{A}_m^{(n)}$ is such an algebra. Then the following equality holds, similarly as usual Clifford algebras,

$$\left(\sum_{i=1}^m\lambda_ie_i\right)^n=\sum_{i=1}^m\lambda_i^ne_i^n\in K \qquad \text{for all } \lambda_i\in K\,.$$

The proof is reduced to the following lemma, by induction on m.

LEMMA. Let K be a field containing a primitive n-th root ω of 1 and $\mathcal{A}$ an algebra over K. Then the equality $xy=\omega yx$ $(x,y\in\mathcal{A})$ implies $(x+y)^n=x^n+y^n$.

7.6. A remark on algebra extensions of non-abelian groups.

In § 6.2, we saw that there exist always central simple algebra extensions of finite abelian groups of symmetric type. There exist also those extensions of some solvable groups (Iwahori-Matsumoto [15]). However, for many kinds of non-abelian groups, there is no central simple algebra extension. In the following, for the sake of simplicity, we assume that K is an algebraically closed field of characteristic 0. Then we have

PROPOSITION 7.5. *Let $\mathfrak{H}_1$ be a non-abelian finite group satisfying one of the following conditions. Then any algebra extension of $\mathfrak{H}_1\times\mathfrak{H}_2$ over K where $\mathfrak{H}_2$ is an arbitrary finite group, is not simple.*

1) $\mathrm{H}^2(\mathfrak{H}_1, K^*)=\{1\}$

2) $\mathfrak{H}_1=\mathfrak{H}_1'$, *and there is no simple algebra extension of* $\mathfrak{H}_1$ *over* K.

3) *There exists an element* P *in* $\mathfrak{H}_1'$ *such that* $\mathrm{H}^2(\mathfrak{Z}_P, K^*)=\{1\}$ *where* $\mathfrak{Z}_P$ *is the centralizer of* P *in* $\mathfrak{H}_1$.

PROOF. Any one of the three conditions implies that, for any algebra extension $\mathcal{A}_1$ of $\mathfrak{H}_1$, there exists an element $P_1 \neq I$ in $\mathfrak{H}_1'$ which is $\mathcal{A}_1$-normal.[36] Let $\mathcal{A}$ be any algebra extension of $\mathfrak{H}_1 \times \mathfrak{H}_2$ and c the corresponding cohomology class in $\mathrm{H}^2(\mathfrak{H}_1 \times \mathfrak{H}_2, K^*)$. We take elements $c_1 \in \mathrm{H}^2(\mathfrak{H}_1, K^*)$, $c_2 \in \mathrm{H}^2(\mathfrak{H}_2, K^*)$ and $\varphi \in \mathrm{P}(\mathfrak{H}_1, \mathfrak{H}_2; K^*)$ corresponding to c (Cf. Theorem 2.1.), and let $\mathcal{A}_1$ be the algebra extension of $\mathfrak{H}_1$ corresponding to c_1. Then, as mentioned above, there exists an element $P_1 \neq I$ in $\mathfrak{H}_1'$ which is $\mathcal{A}_1$-normal. It is sufficient to prove that $P_1 \times I \in \mathfrak{H}_1 \times \mathfrak{H}_2$ is $\mathcal{A}$-normal. Let f be a normalized cocycle in c and f_i the corresponding cocycles in c_i ($i=1, 2$). Then, for $Q_1 \times Q_2 \in \mathfrak{Z}_{P_1 \times I} = \mathfrak{Z}_{P_1} \times \mathfrak{H}_2$, we have

$$
\begin{aligned}
& f(P_1 \times I,\ Q_1 \times Q_2)\, f(Q_1 \times Q_2, P_1 \times I)^{-1} \\
&= f_1(P_1, Q_1)\, f_2(I, Q_2)\, \varphi(P_1, Q_2)\, f_1(Q_1, P_1)^{-1} f_2(Q_2, I)^{-1} \varphi(Q_1, I)^{-1} \\
&= \varphi(P_1, Q_2)\,.
\end{aligned}
$$

Since P_1 is contained in $\mathfrak{H}_1'$, we have $\varphi(P_1, Q_2)=1$. Therefore $P_1 \times I$ is $\mathcal{A}$-normal. This completes the proof.

Applying the above proposition, it follows that $\mathfrak{A}_n \times \mathfrak{H}$ $(n \geqq 5)$ *and* $\mathfrak{S}_n \times \mathfrak{H}$ $(n \geqq 3)$ *have no simple algebra extension where* $\mathfrak{A}_n$ *is the alternating group,* $\mathfrak{S}_n$ *is the symmetric group of degree* n *and* $\mathfrak{H}$ *is an arbitrary finite group.* In fact, $\mathfrak{A}_n$ $(n \geqq 5)$ satisfies the condition 2) since the order of $\mathfrak{A}_n$ is not a square, and $\mathfrak{S}_n$ $(n \geqq 3)$ satisfies the condition 3) for $P=(1, 2, \cdots, n)$ (if n is odd) or $P=(1, 2, \cdots, n-1)$ (if n is even). Note that $\mathfrak{Z}_P$ is a cyclic group and K is algebraically closed.

REMARK 1. There exists a simple algebra extension of $\mathfrak{A}_4 \times \mathfrak{A}_3$ (see [15]).

REMARK 2. $\mathfrak{A}_n$ and $\mathfrak{S}_n$ $(n \geqq 4)$ don't satisfy the condition 1) of Proposition 7.5 (see [3]).

University of Tokyo

Bibliography.

[1] I. Schur, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. für Math., **127** (1904), 20-50.

[2] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, ibid., **132** (1907), 85-137.

[3] I. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe

36) From 3), it follows that any 2-cocycle f of $\mathfrak{H}_1$ induces a 2-coboundary of $\mathfrak{Z}_P$, whence $f_P=1$.

durch gebrochene lineare Substitutionen, ibid., **139** (1911), 155-250.
[4] R. Frucht, Über die Darstellung endlicher Abelscher Gruppen durch Kollineationen, ibid., **166** (1931), 16-29.
[5] K. Asano, Über die Darstellungen einer endlichen Gruppe durch reelle Kollineationen, Proc. Imp. Acad. Japan, **9** (1933), 574-576.
[6] M. Tazawa, Über die Darstellung der endlichen verallgemeinerten Gruppen, Sci. Rep. Tôhoku Univ., 1. s. **23** (1934), 76-88.
[7] K. Asano und K. Shôda, Zur Theorie der Darstellung einer endlichen Gruppe durch Kollineationen, Comp. Math., **2** (1935), 230-240.
[8] T. Nakayama und K. Shôda, Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen, Jap. J. Math., **12** (1935), 109-122.
[9] K. Asano, M. Osima and M. Takahasi, Über die Darstellung von Gruppen durch Kollineationen in Körper der Charakteristik p, Proc. Phy.-Math. Soc. Japan, 3. s. **19** (1937), 199-209.
[10] Y. Kawada, Über die Überlagerungsgruppe und die stetige projektive Darstellung topologischer Gruppen, Jap. J. Math., **17** (1940). 139-164.
[11] S. Eilenberg and S. MacLane, Cohomology theory in abstract groups. I., Ann. Math., **48** (1947), 51-78.
[12] G. Hochschild and J.-P. Serre, Cohomology of group extensions, Trans. Amer. Math. Soc., **74** (1953), 110-134.
[13] R. Frucht, Zur Darstellung endlicher Abelscher Gruppen durch Kollineationen, Math. Zeit., **63** (1955), 145-155.
[14] G. W. Mackey, Unitary representations of group extensions. I., Acta Math., **99** (1958), 265-311.
[15] N. Iwahori and H. Matsumoto, Several remarks on projective representations of finite groups, this Journal.

(Received November 1, 1963)