DIRECT DECOMPOSITIONS OF GALOIS ALGEBRAS

KATSUHIKO MASUDA

(Received April 26, 1952)

In his article "Invariante Kennzeichnung Galoisscher Körper mit vorgegebener Galoisgruppe" [1] H. Hasse established the important concepts of Galois algebras and factor systems. (We call them in the following respectively Hasse's Galois algebras and Hasse factor systems.)

The aim of the present article is to give a characterization of those Hasse factor systems which are associated with Galois fields.

We define Galois algebras more generally than Hasse, as T. Nakayama did [2], and introduce matrix systems associated with them. The generalization simplifies the calculations necessary to solve the above stated problem about Hasse factor systems.

The present work was done while I was a student of Prof. T. Tannaka and I wish to acknowledge my deep indebtedness to him.

1. Let G be a finite group of order n, Ω be a field with characteristic p and $\mathfrak{G}$ be the groupring $G(\Omega)$ of G over Ω. Let K be an algebra, not necessarily associative, having G as a group of automorphisms. We call K a Galois algebra over Ω with Galois group G, if K is as $\mathfrak{G}$-right module isomorphic to $\mathfrak{G}$ itself (i. e. if K possesses a normal basis).

Now we construct a certain Galois algebra $\mathfrak{E}$ over Ω with Galois group G as follows. We associate a symbol e_σ with each element σ of G, construct an algebra $\mathfrak{E}$ over Ω with a basis $\{e_\sigma ; \sigma \in G\}$ such that e_σ's are mutually orthogonal idempotents, and define operations of G in $\mathfrak{E}$ by

$$e_\sigma^\tau = e_{\sigma\tau}$$

$$\Big(\sum_{\sigma\in G}\alpha_\sigma e_\sigma\Big)^\tau = \sum_{\sigma\in G}\alpha_\sigma e_\sigma^\tau \qquad \text{for each } \sigma,\ \tau \in G, \tag{1}$$

where α_σ's are coefficients in Ω. Then $\mathfrak{E}$ becomes an associative, commutative and semisimple Galois algebra over Ω with Galois group G.

We suppose from now that n is not divisible by p and absolute irreducible representations of G are obtained in Ω.

Let r denote the number of different irreducible representations of G and X denote the set of those r irreducible characters. For each element ψ of X we choose arbitrarily an irreducible representation A_ψ in Ω with ψ as character. Let f_ψ denote the degree of A_ψ. Then the following two propositions

1) Crelle J., 187(1949).

2) T. NAKAYAMA, Construction and characterization of Galois Algebras with given Galois group, Nagoya Math. J., 1(1950).

hold.

PROPOSITION 1. *The coefficients of r matrices* $\left\{\sum_{\sigma\in G} A_{\psi}(\sigma^{-1})e_{\sigma};\ \psi\in X\right\}$ *form a bassis of* $\mathfrak{E}$ *over* Ω.

PROPOSITION 2. *Let A be an arbitrary representation of G in* Ω, *not necessarily irreducible, of degree f, and P be such a regular matrix of degree f with coefficients in* Ω *that*

$$A(\sigma)=P^{-1}\begin{pmatrix} A_{\psi_1}(\sigma) & & 0 \\ & A_{\psi_2}(\sigma) & \\ 0 & & \ddots \end{pmatrix}P \qquad \text{for each } \sigma\in G, \tag{2}$$

where ψ_i*'s are elements of X. Let N be such a matrix with coefficients in* $\mathfrak{E}$ *that*

$$N^{\sigma}=A(\sigma)N \qquad \text{for each } \sigma\in G. \tag{3}$$

Then there exists one and only one matrix C with coefficients in Ω *such that*

$$N=\Big(\sum_{\sigma\in G} A(\sigma^{-1})e_{\sigma}\Big)C. \tag{4}$$

Proposition 1 is obtained from the linear independency of representations[3], Proposition 2 is easily seen from Proposition 1 and the fact that we can use the theory of determinants for matrices with coefficients in $\mathfrak{E}$, because of the commutativity and associativity of $\mathfrak{E}$.

Nowt let K be an arbitrary Galois algebra over Ω, not necessarily associative, with Galois group G and with a normal basis $\{u_{\sigma};\ \sigma\in G\}$. Then the following propositions hold as in $\mathfrak{E}$.

PROPOSITION 3. *The coefficients of r matrices* $\left\{\sum_{\sigma\in G} A_{\psi}(\sigma^{-1})u_{\sigma};\ \psi\in X\right\}$ *form a basis of K over* Ω.

PROPOSITION 4. *Let A and P be as in Proposition 2 and N be a matrix with coefficients in K such that*

$$N^{\sigma}=A(\sigma)N \qquad \text{for each } \sigma\in G. \tag{5}$$

Then there exists one and only one such matrix D with coefficients in Ω *that*

$$N=\Big(\sum_{\sigma\in G} A(\sigma^{-1})u_{\sigma}\Big)D. \tag{6}$$

Proposition 3 is clear by Proposition 1, for the one to one correspondence

$$e_{\sigma}\leftrightarrow n_{\sigma} \qquad \text{for each } \sigma\in G. \tag{7}$$

3) BURNSIDE's theorem, cf. H. WEYL, Gruppentheorie und Quantenmechanik, Chap. III.

between the normal basis $\{e_\sigma ; \sigma \in G\}$ of $\mathfrak{E}$ and that $\{u_\sigma ; \sigma \in G\}$ of K induces a $\mathfrak{G}$-right isomorphism between $\mathfrak{E}$ and K. Let N^* denote the matrix with coefficients in $\mathfrak{E}$ which corresponds to N in the above correspondence (7). Then N^* satisfies the conditions of Proposition 2, whence there exists a matrix D with coefficients in Ω such that

$$N^* = \Big(\sum_{\sigma\in G} A(\sigma^{-1})e_\sigma\Big)D. \tag{8}$$

According to the $\mathfrak{G}$-right isomorphism determined by (7), we obtain

$$N = \Big(\sum_{\sigma\in G} A(\sigma^{-1})u_\sigma\Big)D, \tag{9}$$

such matrix D is determined uniquely from (8).

Let $\{C_{\chi,\varphi} ; \chi, \varphi \in X\}$ be a system of r^2 matrices with coefficients in Ω, where $C_{\chi,\varphi}$ is a matrix of degree $f_\chi \cdot f_\varphi$ arbitrarily associated with each pair of elements χ, φ of X. $\{A_\psi ; \psi \in X\}$ is a system of r irreducible representations of G in Ω. We call each pair of such two systems $\{A_\psi ; \psi \in X\}$ and $\{C_{\chi,\varphi} ; \chi, \varphi \in X\}$ a structure of Galois algebra over Ω with Galois group G, or simply a Galois structure of G over Ω.

We call that a Galois structure $[\{A_\psi ; \psi \in X\}, \{C_{\chi,\varphi} ; \chi, \varphi \in X\}]$ of G over Ω is associated with a Galois algebra K over Ω with Galois group G, if there exist two systems of matrices $\{W_\psi ; \psi \in X\}$ and $\{P_{\chi,\varphi} ; \chi, \varphi \in X\}$ such that $\{W_\psi ; \psi \in X\}$ is a factor basis of K over Ω associated with $\{A_\psi ; \psi \in X\}$, i.e. the coefficients of r matrices of $\{W_\psi ; \psi \in X\}$ form a basis of K over Ω,

$$W_\psi^\sigma = A_\psi(\sigma)\, W_\psi \qquad \text{for each } \sigma \in G,\ \psi \in X, \tag{10}$$

and

$$W_\chi \times W_\varphi = P_{\chi,\varphi}^{-1}\begin{pmatrix} W_{\lambda_1(\chi,\varphi)} & & 0 \\ & W_{\lambda_2(\chi,\varphi)} & \\ 0 & & \ddots \end{pmatrix} P_{\chi,\varphi}\, C_{\chi,\varphi} \qquad \text{for each } \chi, \varphi \in X \tag{11}$$

where $\lambda_i(\chi, \varphi)$ are elements of X determined by this relation (11) and $\times$ denotes Kronecker product.

We say that Galois structures $\mathfrak{S}$ and $\mathfrak{S}'$ of G over Ω are equivalent, written

$$\mathfrak{S} \sim \mathfrak{S}', \tag{12}$$

if and only if $\mathfrak{S}$ and $\mathfrak{S}'$ are associated with isomorphic Galois algebras over Ω with Galois group G. From Proposition 3 and Proposition 4 follows that the classes of equivalent Galois structures of G over Ω are in one to one correspondence with classes of isomorphic Galois algebras over Ω with Galois group G.

2. The following theorem holds without the assumptions for G and Ω stated in § 1.

THEOREM 1[4]. *Let K be an associative, commutative and semisimple algebra over a field Ω and have G as an automorphism group. Then K is a Galois algebra over Ω with Galois group G, if and only if every element of G leaves Ωe elementweise invariant and every element of K left invariant by all elements of G belongs to Ωe and the order n of G is equal to $[K:\Omega]$[5], where e denotes the unit element of K.*

PROOF. As K is an associative, commutative and semisimple algebra, K is a direct sum of a certain number of fields, say $K_1, K_2, \cdots, K_m$. Then

$$e = e_1 + e_2 + \cdots + e_m, \tag{13}$$

where e_i denotes the unit element of K_i for $i = 1, 2, \cdots, m$. Let H denote the subgroup of G which consists of all elements of G that leave e_1 invariant. Let $\sigma_1, \sigma_2 \cdots, \sigma_{m'}$ be a complete system of representatives of right cosets of G by H and especially σ_1 be the unit element of G. Now suppose that G characterizes Ωe as the totality of elements that are left invariant by G. Then follows

$$m = m' \tag{14}$$

and $\sigma_j^{-1} H \sigma_j$ induces an automorphism in K_j and

$$e_1^{\sigma_j} = e_j, \quad K_1^{\sigma_j} = K_j, \tag{15}$$

if we permute the suffices of $\sigma_1, \sigma_2, \cdots, \sigma_m$ suitably. Moreover it is easy to see that the set of elements of K_j left invariant by $\sigma_j^{-1} H \sigma_j$ is Ωe_j. Then K_j is a separable Galois extension field of Ωe_j, having exactly $\sigma_j^{-1} H \sigma_j$ as its Galois group from the supposition that the rank of K over Ω is equal to the order of G. As K_1 is a Galois extension over Ωe_1 there exists a normal basis $\{\theta_1^{\tau}; \tau \in H\}$. Then $\{\theta_1^{\tau\sigma_j}; \tau \in H, j = 1, 2. \cdots, m\}$ becomes clearly a normal basis of K over Ω, so K is a Galois algebra over Ω with Galois group G. The rest of Theorem 1 is trivial.

Let K be a Galois algebra over Ω with Galois group G, and H be a subgroup of G. Let $\sigma_1, \sigma_2, \cdots, \sigma_m$ be a complete system of representatives of right cosets of G by H and σ_1 be especially the unit of G. We say that K has a direct decomposition with respect to H, if K is a direct sum of m algebras $K_1, K_2, \cdots, K_m$, such that K_1 is a Galois algebra over Ω with Galois group H and

$$K_j = K_1^{\sigma_j} \qquad \text{for } j = 1, 2, \cdots m, \tag{16}$$

where suffices of K_j are chosen suitably. We call then K_1 its component for H in the decompsoition. Here we state two lemmas which also hold without the suppositions for G and Ω stated in §1.

The following two lemmas are easy to verify.

---

4) A similar theorem was proved formerly by A. A. Albert.

5) The totality of automorphisms of K leaving Ωe elementweis invariant is generally larger than G. It coinsides with G if and only if K is a field.

LEMMA 1. *Let H be a subgroup of G, L be a Galois algebra over Ω with Galois group H. Then there exists a Galois algebra over Ω with Galois group G that has a decomposition with respect to H and has L as component for H.*

LEMMA 2. *Let K be an associative, commutative and semisimple Galois algebra over Ω with Galois group G. Then K is a field, if and only if K does not have a direct decomposition with respect to any proper subgroup of G.*

3. Let G be a finite group of order n, H be a subgroup of G and Ω be a field with characteristic p. Suppose that n is not divisible by p and irreducible representations of G and H are obtained in Ω. Denote by X and Y respectively the set of irreducible characters of G and H in Ω. We call that a Galois structure $[\{A_\psi;\ \psi \in X\},\ \{C_{\chi,\varphi};\ \chi,\ \varphi \in X\}]$ of G over Ω has a decomposition with respect to H, if there exists at least one Galois structure $[\{B_\nu;\ \nu \in Y\},\ \{D_{\lambda,\mu};\ \lambda,\ \mu \in Y\}]$ of H over Ω that satisfies the following two conditions.

CONDITION 1. The restriction on H of each A_ψ ($\psi \in X$) is a direct sum of some representations belonging to $\{B_\nu;\ \nu \in Y\}$, that is

$$A_\psi(\tau) = \begin{pmatrix} B_{(\psi,1)}(\tau) & & 0 \\ & B_{(\psi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} \qquad \text{for each } \tau \in H, \tag{17}$$

where $(\psi,1)$, $(\psi,2)$, $\ldots$ denote some elements of Y.

CONDITION 2. $C_{\chi,\varphi}$ for each χ, φ is related to matrices belonging to $\{D_{\lambda,\mu};\ \lambda,\ \mu \in Y\}$ with above defined symbols (ψ, i) as follows,

$$C_{\chi,\varphi} = T^{-1}_{\chi,\varphi} \begin{pmatrix} D_{(\chi,1),(\varphi,1)} & & & & & \\ & D_{(\chi,1),(\varphi,2)} & & & & \\ & & \ddots\ D_{(\chi,i),(\varphi,j)} & & & \\ & & & D_{(\chi,i),(\varphi,j+1)} & & \\ & & & & \ddots\ D_{(\chi,i+1),(\varphi,1)} & \\ & & & & & \ddots \end{pmatrix} T_{\chi,\varphi}, \tag{18}$$

where $T_{\chi,\varphi}$ is a regular transposition matrix in Ω such that

$$A_\chi(\tau)\times A_\varphi(\tau) = T^{-1}_{\chi,\varphi} \begin{pmatrix} B_{(\chi,1)}(\tau)\times B_{(\varphi,1)}(\tau) & & 0 \\ & B_{(\chi,1)}(\tau)\times B_{(\chi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} T_{\chi\cdot\varphi}$$

for $\tau \in H$.

We denote the right-hand matrix by $D_{\chi,\varphi}$, and call $[\{B_\nu;\ \nu \in X\},\ \{D_{\lambda,\mu};\ \lambda,\ \mu \in X\}]$ the component Galois structure in the decomposition with respect to H.

The next thorem is the main result of the present article.

THEOREM 2. *Let K be a Galois algebra over Ω with Galois group G. K has* *a direct decomposition with respect to H, if and only if there exists at least one Galois structure of G over Ω associated with K having a decomposition with respect to H.*

PROOF. Let $\sigma_1, \sigma_2, \dots, \sigma_m$ be a complete system of representatives of right cosets of G by H, σ_1 being the unit element of G,

$$m = [G:H]. \tag{19}$$

Let K_1 be the component for H and suppose

$$K_1^{\sigma_j} = K_j \qquad \text{for } j = 1, 2, \dots, m. \tag{20}$$

Let θ_1 be such an element of K_1 that $\{\theta_1^{\tau}; \tau \in H\}$ is a normal basis of K_1. Then

$$\theta_1^{\sigma_j} \in K_j, \tag{21}$$

and $\{\theta_1^{\tau\sigma_j}; \tau \in H, j = 1, 2, \dots, m\}$ is a normal basis of K over Ω. We take a factor basis $\{W_\psi; \psi \in X\}$ such that

$$W_\psi = \sum_{j=1}^{m}\sum_{\tau\in H} A_\psi(\sigma_j^{-1}\tau^{-1})\,\theta_1^{\tau\sigma_j} \tag{22}$$

Let $P_{\chi,\varphi}$ be a regular matrix with coefficients in Ω of degree $f_\chi \cdot f_\varphi$ such that

$$A_\chi \times A_\varphi = P_{\chi,\varphi}^{-1}\begin{pmatrix} A_{(\chi,\varphi,1)} & & 0 \\ & A_{(\chi,\varphi,2)} & \\ 0 & & \ddots \end{pmatrix} P_{\chi,\varphi}, \tag{23}$$

where (χ, φ, i)'s are elements of X.

Then

$$\begin{aligned} W_\chi \times W_\varphi &= \Big(\sum_{j=1}^{m}\sum_{\tau\in H} A_\chi(\sigma_j^{-1}\tau^{-1})\,\theta^{\tau\sigma_j}\Big) \times \Big(\sum_{j=1}^{m}\sum_{\tau\in H} A_\varphi(\sigma_j^{-1}\tau^{-1})\theta_1^{\tau\sigma_j}\Big) \\ &= \Big\{\sum_{j=1}^{m}\Big(A_\chi(\sigma_j^{-1})\sum_{\tau\in H} A_\chi(\tau^{-1})\theta_1^{\tau\sigma_j}\Big\} \times \Big\{\sum_{j=1}^{m}\Big(A_\varphi(\sigma_j^{-1})\sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^{\tau\sigma_j}\Big)\Big\} \\ &= \sum_{j=1}^{m}\Big(\Big\{A_\chi(\sigma_j^{-1})\sum_{\tau\in H} A_\chi(\tau^{-1})\theta_1^{\tau\sigma_j}\Big\} \times \Big\{A_\varphi(\sigma_j^{-1})\sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^{\tau\sigma_j}\Big\}\Big) \\ &= \sum_{j=1}^{m}\Big(A_\chi \times A_\varphi(\sigma_j^{-1})\cdot\Big\{\sum_{\tau\in H} A_\chi(\tau^{-1})\theta_1^{\tau\sigma_j} \times \sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^{\tau\sigma_j}\Big\}\Big). \end{aligned}$$

We determine $C_{\chi,\varphi}$ by

$$W_\chi \times W_\varphi = P_{\chi,\varphi}^{-1}\, W_{\chi,\varphi}\, P_{\chi,\varphi}\, C_{\chi,\varphi}, \tag{25}$$

where

$$W_{\chi,\varphi} = \sum_{j=1}^{m}\sum_{\tau\in H} A_{\chi,\varphi}(\sigma_j^{-1}\tau^{-1})\theta_1^{\tau\sigma_j} \tag{26}$$

and $A_{\chi,\varphi}$ denotes

$$(27) \qquad A_{\chi,\varphi} = P_{\chi,\varphi}\, A_\chi \times A_\varphi\, P_{\chi,\varphi}^{-1} = \begin{pmatrix} A_{(\chi,\varphi,1)} & & 0 \\ & A_{(\chi,\varphi,2)} & \\ 0 & & \ddots \end{pmatrix}.$$

Then $C_{\chi,\varphi}$ is a matrix with coefficients in Ω of degree $f_\chi \cdot f_\varphi$ and $[\{A_\psi ; \psi \in X\}, \{C_{\chi,\varphi} ; \chi, \varphi \in X\}]$ is a Galois structure of G over Ω associated with K.

Comparing the K_1-components of (24) we obtain

$$(28) \qquad A_\chi \times A_\varphi(\sigma_1^{-1}) \cdot \Big(\sum_{\tau\in H} A_\chi(\tau^{-1})\theta_1^\tau \times \sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^\tau\Big)$$
$$= P_{\chi,\varphi}^{-1}\Big(A_{\chi,\varphi}(\sigma_1^{-1}) \sum_{\tau\in H} A_{\chi,\varphi}(\tau^{-1})\theta_1^\tau\Big)\, P_{\chi,\varphi}\, C_{\chi,\varphi}\ ,$$

that is,

$$(29) \qquad \sum_{\tau\in H} A_\chi(\tau^{-1})\theta_1^\tau \times \sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^\tau = P_{\chi,\varphi}^{-1} \sum_{\tau\in H} A_{\chi,\varphi}(\tau^{-1})\theta_1^\tau\, P_{\chi,\varphi}\, C_{\chi,\varphi}.$$

From now on we suppose, without any loss of generality of the proof, that $\{A_\psi ; \psi \in X\}$ satisfies the Condition 1, that is

$$(30) \qquad A_\psi(\tau) = \begin{pmatrix} B_{(\psi,1)}(\tau) & & 0 \\ & B_{(\psi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} \qquad \text{for each } \tau \in H.$$

Let $Q_{\lambda,\mu}$ be a matrix with coefficients in Ω of degree $f_\lambda \cdot f_\mu$ such that

$$(31) \qquad Q_{\lambda,\mu}(B_\lambda(\tau) \times B_\mu(\tau))Q_{\lambda,\mu}^{-1} = \begin{pmatrix} B_{(\lambda,\mu,1)}(\tau) & & 0 \\ & B_{(\lambda,\mu,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} \text{for each } \tau \in H,\ \lambda, \mu \in Y,$$

where (λ, μ, i)'s are some elements of Y. We denote the right-hand matrix by $B_{\lambda,\mu}(\tau)$; We define a quadratic matrix $D_{\lambda,\mu}$ for each $\lambda, \mu \in Y$ by

$$(32) \qquad \sum_{\tau\in H} B_\lambda(\tau^{-1})\theta_1^\tau \times \sum_{\tau\in H} B_\mu(\tau^{-1})\theta_1^\tau = Q_{\lambda,\mu}^{-1}\Big(\sum_{\tau\in H} B_{\lambda,\mu}(\tau^{-1})\theta_1^\tau\Big)Q_{\lambda,\mu}\, D_{\lambda,\mu}.$$

Then $D_{\lambda,\mu}$ is a quadratic matrix with coefficients in Ω of degree $f_\lambda \cdot f_\mu$. $[\{B_\nu ; \nu \in Y\}, \{D_{\lambda,\mu} ; \lambda, \mu \in Y\}]$ is clearly a Galois structure of H over Ω. We construct a matrix $D_{\chi,\varphi}$ for each $\chi, \omega \in X$ as follows.

$$(33) \qquad D_{\chi,\varphi} = \begin{pmatrix} D_{(\chi,1),(\varphi,1)} & & 0 \\ & D_{(\chi,1),(\varphi,2)} & \\ 0 & & \ddots \end{pmatrix}.$$

Then

$$(34) \quad \Big(\sum_{\tau\in H} A_\chi(\tau^{-1})\theta^\tau\Big) \times \Big(\sum_{\tau\in H} A_\varphi(\tau^{-1})\theta_1^\tau\Big) = T_{\chi,\varphi}^{-1} Q_{\chi,\varphi}^{-1} \sum_{\tau\in H} B_{\chi,\varphi}(\tau^{-1})\theta_1^\tau Q_{\chi,\varphi}\, D_{\chi,\varphi} T_{\chi,\varphi},$$

where

$$(35) \qquad Q_{\chi,\varphi} = \begin{pmatrix} Q_{(\chi,1),(\varphi,1)} & & 0 \\ & Q_{(\chi,1),(\varphi,2)} & \\ 0 & & \ddots \end{pmatrix}$$

(36) $$B_{\chi,\varphi}(\tau) = \begin{pmatrix} B_{(\chi,1),(\varphi,1)}(\tau) & & 0 \\ & B_{(\chi,1),(\varphi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix}.$$

The diagonal parts are constructed lexicographically.

From (29) and (34) we obtain without difficulty

(37) $$C_{\chi,\varphi} = T^{-1}_{\chi,\varphi} D_{\chi,\varphi} T_{\chi,\varphi}[6].$$

Suppose now conversely that a Galois structure $[\{A_\psi ; \psi \in X\}, \{C_{\chi,\varphi} : \chi, \varphi \in X\}]$ has a decomposition with respect to H. Let the decomposition be as follows;

(38) $$A_\psi(\tau) = \begin{pmatrix} B_{(\psi,1)}(\tau) & & 0 \\ & B_{(\psi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} \qquad \text{for each } \tau \in H,\ \psi \in X,$$

and

(39) $$C_{\chi,\varphi} = T^{-1}_{\chi,\varphi} D_{\chi,\varphi} T_{\chi,\varphi} \qquad \text{for each } \chi, \varphi \in X.$$

where $[\{B_\nu ; \nu \in Y\}, \{D_{\lambda,\mu} ; \lambda, \mu \in Y\}]$ is the component Galois structure of H over Ω. Then there exists at least one Galois algebra L with which $[\{B_\nu ; \nu \in Y\}, \{D_{\lambda,\mu} ; \lambda, \mu \in Y\}]$ is associated. We construct a Galois algebra K^* over Ω with Galois group G as Lemma 1 in § 2. From the above proof of the necessity of the condition of Theorem 2 there exists a Galois structure $[\{A_\psi ; \psi \in X\}, \{C'_{\chi,\varphi} ; \chi, \varphi \in X\}]$ of G over Ω associated with K^* possessing a decomposition

(40) $$A_\psi(\tau) = \begin{pmatrix} B_{(\psi,1)}(\tau) & & 0 \\ & B_{(\psi,2)}(\tau) & \\ 0 & & \ddots \end{pmatrix} \qquad \text{for each } \tau \in H,\ \psi \in X,$$

and

(41) $$C'_{\chi,\varphi} = T^{-1}_{\chi,\varphi} D_{\chi,\varphi} T_{\chi,\varphi} \qquad \text{for each } \chi,\ \varphi \in X.$$

Then

(42) $$C_{\chi,\varphi} = C'_{\chi,\varphi},$$

whence

(43) $$K' \cong K,$$

and K has a direct decomposition with respect to H. q. e. d.

Considering the fact for any $\nu \in Y$ there exists at least one character of G whose restriction to H has ν as an irreducible component[7], we obtain the following Corollary.

COROLLARY. *Let a Galois structure $[\{A_\psi ; \psi \in X\}, \{C_{\chi,\varphi} ; \chi, \varphi \in X\}]$ of G over Ω has a decomposition with respect to H and $[\{B_\nu ; \nu \in Y\}, \{D_{\lambda,\mu} ; \lambda, \mu \in Y\}]$ be the component of decomposition. $\{C_{\chi,\varphi} ; \chi, \varphi \in X\}$ is Hasse factor system, if and only if $\{D_{\lambda,\mu} ; \lambda, \mu \in Y\}$ is Hasse factor system.*

4. Now we state some applications of Theorem 2 and Lemmas without

6) Cf. H HASSE (1).

7) FROBENIUS' theorem.

proof.

THEOREM 3. *Let G be a finite group, m denote the least common multiple of the orders of the elements of G. Suppose that Ω is a field with characteristic p, m is not divisible by p and every m-th root of 1 is cotained in Ω. Then an associative, commutative and semisimple Galois algebra K over Ω with Galois group G is a field, if and only if every Galois structure of G over Ω associated with K does not have a decomposition with respect to any proper subgroup of G.*

THEOREM 4. *Let Ω be an algebraic number field, K be a finite Galois extension field of Ω with Galois group G, m denote the least common multiple of orders of all elements of G. Suppose Ω contains every m-th root of 1, $\mathfrak{S}$ be a Galois structure of G over Ω associated with K. Let $\mathfrak{p}$ be a prime ideal of Ω and decompose in K such as*

$$\mathfrak{p} = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$$

where $\mathfrak{P}_i$'s for $i = 1, 2, \ldots g$ are prime ideals in K. The decomposition groups of $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are characterized as minimal groups with respect to which there exists a Galois structure of G over $\Omega_\mathfrak{p}$ equivalent with $\mathfrak{S}$, considered as a structure of G over $\Omega_\mathfrak{p}$ having a decomposition.

This is a generalization of a theorem for Kummer fields.

MATHEMATICAL INSTITUTE, YAMAGATA UNIVERSITY, YAMAGATA.