CONSTRUCTION AND CHARACTERIZATION OF GALOIS ALGEBRAS WITH GIVEN GALOIS GROUP

TADASI NAKAYAMA

Recently H. Hasse \(^1\) has given an interesting theory of Galois algebras, which generalizes the well known theory of Kummer fields; an algebra \( \mathcal{A} \) over a field \( \Omega \) is called a Galois algebra with Galois group \( G \) when \( \mathcal{A} \) possesses \( G \) as a group of automorphisms and \( \mathcal{A} \) is \((G, \Omega)\)-operator-isomorphic to the group ring \( G(\Omega) \) of \( G \) over \( \Omega \).\(^2\) On assuming that the characteristic of \( \Omega \) does not divide the order of \( G \) and that absolutely irreducible representations of \( G \) lie in \( \Omega \), Hasse constructs certain \( \omega \)-basis of \( \mathcal{A} \), called factor basis, in accord with Wedderburn decomposition of the group ring and shows that a characterization of \( \mathcal{A} \) is given by a certain matrix factor system which defines the multiplication between different parts of the factor basis belonging to different characters of \( G \). Now the present work is to free the theory from the restriction on the characteristic. We can indeed embrace the case of non-semisimple modular group ring \( G(\Omega) \).

1. Decomposition of group ring.\(^3\) Let \( G \) be a finite group whose absolutely irreducible representations lie in a field \( \Omega \). Let \( \mathbb{G} = G(\Omega) \) be its group ring over \( \Omega \). Let

\[
1 = \sum_{\kappa} \sum_{i,j} e_{ij}^{(\kappa)}
\]

be a decomposition of 1 into a sum of mutually orthogonal primitive idempotent elements in \( \mathbb{G} \), where the left-(or, right-)ideals generated by \( e_{ij}^{(\kappa)} \), are isomorphic while those generated by \( e_{ij}^{(\kappa)} \), \( e_{ji}^{(\lambda)} \) with \( \kappa \neq \lambda \) are not. Let \( e_{ij}^{(\kappa)} \) be, for each \( \kappa \), a corresponding system of matric units. For simplicity’s sake we denote \( e_{ij}^{(\kappa)} \) by \( e^{(\kappa)} \). Let

\[\text{Received December 26, 1949; revised March 5, 1950. The revision was to make the paper into a form of abstract, so as to transfer the original full account, with further supplement, to Crelles Journal according to Prof. Hasse’s kind invitation.}\]

\(^1\) [2].

\(^2\) Hasse demands further that \( \mathcal{A} \) be associative, commutative and, moreover, semisimple.

\(^3\) Cf. e.g. [3].
be an (independent) \( \Omega \)-basis of the right ideal \( e^{(\kappa)} \mathfrak{G} \) taken in accord with a composition series. We have, for \( z \in \mathfrak{G} \),

\[
\mathbf{v}^{(\kappa)} z = V^{(\kappa)}(z) \mathbf{y}^{(\kappa)}
\]

with a representation \( V^{(\kappa)} \) of \( \mathfrak{G} \) in \( \Omega \). We assume that \( e^{(1)} \) corresponds to the 1-representation of \( G \). We can, and shall, take \( \sum_{z \in \mathfrak{G}} z \) for \( f^{(1)} \).

As for the left-ideal \( \mathfrak{G} e^{(\kappa)} \) we take its basis

\[
\mathbf{u}^{(\kappa)} = (e^{(\kappa)}, s^{(\kappa)}_{\mathbf{x}}, \ldots, s^{(\kappa)}_{\mathbf{y}})
\]

in the following more specified manner. Let namely the \( q \)-th residue-module in a composition series of \( \mathfrak{G} e^{(\kappa)} \) correspond to \( e^{(\kappa)(x)} \) (i.e. be isomorphic to \( \mathfrak{G} e^{(\kappa)(x)}/\mathfrak{G} e^{(\kappa)(x)}[\mathfrak{R}] \), where \( \mathfrak{R} \) denotes the radical of \( \mathfrak{G} \)), and take a generator \( r^{(\kappa)(x)} (\in \mathfrak{G}) \) of the residue-module; \( r^{(\kappa)(x)} \) may be taken from \( e^{(\kappa)(x)} \mathfrak{G} e^{(\kappa)} \), and we really employ \( e^{(\kappa)} \) as \( r^{(\kappa)} \). Then

\[
((x^{(\kappa)}, c^{(\kappa)}_{\mathbf{x}}, \ldots), (x^{(\kappa)(x)}, c^{(\kappa)(x)}_{\mathbf{x}}, \ldots))
\]

forms a basis of \( \mathfrak{G} e^{(\kappa)} \), which we take for \( \mathbf{u}^{(\kappa)} \) in (4).

Now we introduce a matrix

\[
\mathbb{X}^{(\kappa)} = (y^{(\kappa)}, s^{(\kappa)}_{\mathbf{x}} y^{(\kappa)}, \ldots, s^{(\kappa)}_{\mathbf{y}} y^{(\kappa)} y^{(\kappa)})
\]

in \( \mathfrak{G} \); it is the transpose of the Kronecker product, so to speak, of the transposes of \( \mathbf{u}^{(\kappa)}, \mathbf{v}^{(\kappa)} \). Denote the matrix consisting of the first \( f^{(\kappa)} \) columns of \( \mathbb{X}^{(\kappa)} \) by \( \mathbb{S}^{(\kappa)} \), i.e.

\[
\mathbb{S}^{(\kappa)} = (y^{(\kappa)}, c^{(\kappa)}_{\mathbf{x}} y^{(\kappa)}, \ldots, c^{(\kappa)}_{\mathbf{f}^{(\kappa)}} y^{(\kappa)})
\]

We have

\[
\mathbb{X}^{(\kappa)} = \mathbb{S}^{(\kappa)}
\]

with a matrix \( \mathbb{S}^{(\kappa)} \) in \( \Omega \). Here

\[
\begin{pmatrix}
\mathbb{S}^{(\kappa)} \\
\mathbb{S}^{(\kappa)(x)} \\
\vdots
\end{pmatrix}
= K^{(\kappa)*} 
\begin{pmatrix}
\mathbb{S}^{(1)} \\
\mathbb{S}^{(1)(x)} \\
\vdots
\end{pmatrix}
\]

with matrices \( K^{(\kappa)}, K^{(\kappa)*} \) possessing one 1 in each column or row respectively. Thus
Galois algebras with given Galois group

\[ \mathfrak{F}(\kappa) = S(\kappa)K(\kappa) : K(\kappa) \]

If \( \mathfrak{G} \) is any column of elements of \( \mathfrak{G} \) satisfying \( \mathfrak{G}z = V(\kappa)(z)\mathfrak{G} \), then there exists an element \( x \) in \( \mathfrak{G} \) such that \( \mathfrak{G} = x\mathfrak{G} \). Hence \( \mathfrak{G} = \mathfrak{F}(\kappa)X \) with a column \( X \) in \( \mathfrak{G} \); in fact \( X \) is the first column of the matrix corresponding to \( x \) in the representation of \( \mathfrak{G} \) defined by \( \mathfrak{G}e^x \) with respect to our basis \( u^x \).

Now, Kronecker products of \( V(\kappa) \) are decomposed, directly, into certain numbers of \( V(\kappa) \). Thus

\[ V(\kappa) \times V(\kappa) = P_{\kappa,\kappa} \begin{pmatrix} V(w_1(\kappa,\lambda,\mu)) \\ \vdots \\ V^{(l)} \end{pmatrix} P_{\kappa,\kappa} \]

with a non-singular matrix \( P_{\kappa,\kappa} \) in \( \mathfrak{G} \). There is a matrix \( G_{\kappa,\kappa} \) possessing one 1 in each column such that

\[ \begin{pmatrix} V(w_1(\kappa,\nu,\lambda)) \\ \vdots \\ V^{(l)} \end{pmatrix} = G'_{\kappa,\nu} \]

\[ \begin{pmatrix} V^{(l)} \\ \vdots \\ V^{(l)} \end{pmatrix} \]

We have next

\[ V(\lambda) \times V(\kappa) = J_{\kappa,\lambda}^{-1}(V(\kappa) \times V(\lambda))J_{\kappa,\lambda} \]

with permutation matrix \( J_{\kappa,\lambda} \). Further we may assume

\[ \omega(\lambda, \kappa) = \omega(\kappa, \lambda), \quad G_{\kappa,\lambda} = G_{\kappa,\kappa}, \quad \text{and} \quad P_{\kappa,\kappa} = P_{\kappa,\kappa}J_{\kappa,\lambda}. \]

Finally we quote the following particular case of the Nesbitt-Brauer-Nakayama orthogonality relation

\[ \sum_{\gamma \in \mathfrak{G}} V^{(l)}(z) = \begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix} \quad (\gamma \neq 0), \quad \sum_{\gamma \in \mathfrak{G}} V^{(l)}(z) = 0 \quad (\kappa \neq 1). \]

2. Galois algebra. Let \( \mathcal{A} \) be an algebra, not necessarily associative, over \( \mathfrak{G} \).

---

4) See [5].
5) See [1], [4].
which has \( G \) as a group of automorphisms. We call \( \mathcal{A} \) a Galois algebra, with Galois group \( G \), when the right \( \mathcal{O}(= G(\mathcal{O})) \)-module \( \mathcal{A} \) is isomorphic to \( \mathcal{O} \) itself (i.e. when \( \mathcal{A} \) possesses a normal basis). Let, with such a Galois algebra \( \mathcal{A} \), \( \sim \) denote an isomorphism of \( \mathcal{O} \) and \( \mathcal{A} \). We have

\[
\mathcal{A}^{(x)} z = V^{(x)}(z) \mathcal{A}^{(x)}
\]

for \( z \in \mathcal{O} \). So \((\mathcal{A}^{(x)} \times \mathcal{A}^{(y)}) z = (V^{(x)} \times V^{(y)})(z)(\mathcal{A}^{(x)} \times \mathcal{A}^{(y)})\), or

\[
P_{x,\lambda}(\mathcal{A}^{(x)} \times \mathcal{A}^{(y)}) z = \begin{pmatrix} V^{(w(x,\lambda))}(z) \\ \cdot \\ \cdot \end{pmatrix} P_{y,\lambda}(\mathcal{A}^{(x)} \times \mathcal{A}^{(y)}).
\]

Hence, from an observation in 1 (and the isomorphism property of \( \sim \)),

\[
P_{x,\lambda}(\mathcal{A}^{(x)} \times \mathcal{A}^{(y)}) = \begin{pmatrix} \mathcal{A}^{(x)}_{w(x,\lambda)} \\ \cdot \\ \cdot \end{pmatrix} P_{y,\lambda}A_{x,\lambda} = G'_{x,\lambda}
\]

i.e.

\[
\mathcal{A}^{(x)} \times \mathcal{A}^{(y)} = P_{x,\lambda}G'_{x,\lambda}
\]

\[
\begin{pmatrix} S^{(1)} \\ \cdot \\ \cdot \end{pmatrix} \begin{pmatrix} K^{(1)} \\ \cdot \end{pmatrix} = \begin{pmatrix} (I_k \times \mathcal{A}^{(1)}) \\ \cdot \end{pmatrix}
\]

\[(17)\]

with uniquely determined matrix \( A_{x,\lambda} \) of type \((v(x)v(y), f(x)f(y)) \) in \( \mathcal{O} \), \( I_k \) being unit matrix of degree \( k \). Taking \( A_{x,\lambda} \) for each pair \((x,\lambda)\) we obtain a system \( \{A_{x,\lambda}; \ x, \lambda = 1, 2, \ldots, k\} \) of matrices in \( \mathcal{O} \).

Conversely any system \( \{A_{x,\lambda}\} \), with each \( A_{x,\lambda} \) possessing type \((v(x)v(y), f(x)f(y)) \), defines a Galois algebra with Galois group \( G \). Namely, if we introduce

\[g = \sum f(x)v(x)\] elements, arrange them into \( k \) matrices \( \mathcal{A}^{(x)} \) of respective type \((v(x), f(y)) \), define by virtue of (17) an \( \mathcal{O} \)-linear multiplication in the \( \mathcal{O} \)-module \( \mathcal{A} \) spanned by the elements, considered as being independent, and set (16), then we see that \( \mathcal{A} \) becomes a Galois algebra with Galois group \( G \) corresponding to the given system \( \{A_{x,\lambda}\} \).

Now, similar consideration can be made for \( \mathcal{A}^{(x)} \times \mathcal{A}^{(y)} \) too, to give

\[
\mathcal{A}^{(x)} \times \mathcal{A}^{(y)} = P_{x,\lambda}G'_{x,\lambda}
\]

\[
\begin{pmatrix} \mathcal{A}^{(1)} \\ \cdot \\ \cdot \end{pmatrix} G_{x,\lambda}P_{x,\lambda}B_{x,\lambda}
\]

\[(18)\]
with again uniquely determined matrix $B_{\kappa,\lambda}$, of degree $v(\kappa)v(\lambda)$; $A_{\kappa,\lambda}$ is composed of certain $f(\kappa)f(\lambda)$ columns of $B_{\kappa,\lambda}$. Also the system $\{B_{\kappa,\lambda}\}$ characterizes $\mathfrak{A}$, but it must be observed that it can not, in general, be taken arbitrarily, contrary to $\{A_{\kappa,\lambda}\}$. Indeed, elements of $B_{\kappa,\lambda}$ can be expressed linearly by those of $A\$s, the expression depending on $G$ (and $\Omega$) only (but not on $\mathfrak{A}$), which we write in (19)

$$B_{\kappa,\lambda} = B_{\kappa,\lambda}(\{A_{\kappa,\lambda}\}).$$

Let, with our same $\mathfrak{A}$, a second (®-) isomorphism of $\mathfrak{G}$ and $\mathfrak{A}$ be denoted by $\bar{\cdot}$. There exists a regular element $a$ in $\mathfrak{G}$ such that $\bar{x} = \bar{a}x$ ($x \in \mathfrak{G}$). We see that

$$(20) \quad F^{-1}G'_{\kappa,\lambda} = \begin{pmatrix} U^{(1)}(a)^{-1} & \cdots & \cdots & & \cdots \\ & \ddots & \ddots & \ddots & \cdots \\ & & U^{(k)}(a)^{-1} & \cdots & \cdots \end{pmatrix} G_{\kappa,\lambda}B_{\kappa,\lambda}(U^{(1)}(a) \times U^{(k)}(a))$$

plays for $\bar{\mathfrak{G}}(\kappa)$ the roll of $B_{\kappa,\lambda}$ for $\mathfrak{G}(\kappa)$, where $U^{(k)}$ denotes the representation defined by the basis $u^{(k)}$ of $\mathfrak{G}(\kappa)$. Thus:

(Under the assumption that all absolutely irreducible representations of $G$ lie in $\Omega$) to each Galois algebra $\mathfrak{A}$ over $\Omega$ with Galois group $G$ is associated a class of systems $\{A_{\kappa,\lambda}\}$ mutually related by transformation which takes $A_{\kappa,\lambda}$ into the matrix consisting of the $1st, \ldots, f(\lambda)-th, v(\lambda)+1st, \ldots, v(\lambda)+f(\lambda)-th, \ldots$ columns of (20) with $B_{\kappa,\lambda} = B_{\kappa,\lambda}(\{A_{\kappa,\lambda}\})$, a being regular element in $\mathfrak{G}$. Multiplication in $\mathfrak{A}$ is given in terms of $\{A_{\kappa,\lambda}\}$ by (17), and operation of $G$ on $\mathfrak{A}$ by (16). Conversely, any system $\{A_{\kappa,\lambda}\}$ of matrices in $\Omega$, with respective type $(v(\kappa)v(\lambda), f(\kappa)f(\lambda))$, gives rise to a Galois algebra over $\Omega$ with Galois group $G$.  

3. Associativity, commutativity and semisimplicity. If $\mathfrak{A}$ is commutative, then the permutation matrix $J_{\kappa,\lambda}$ in (13) gives also $J^{-1}_{\kappa,\lambda}(\bar{\mathfrak{G}}(\kappa) \times \bar{\mathfrak{G}}(\lambda))J_{\kappa,\lambda} = \bar{\mathfrak{G}}(\kappa) \times \bar{\mathfrak{G}}(\lambda)$. We have then

$$(21) \quad B_{\kappa,\lambda} = J^{-1}_{\kappa,\lambda}B_{\kappa,\lambda}J_{\kappa,\lambda},$$

which gives in fact necessary and sufficient condition for the commutativity of $\mathfrak{A}$; if we take (19) (and perhaps its trivial inverse) into account, the condition can be regarded as being in terms of $\{A_{\kappa,\lambda}\}$. On considering $V(\kappa) \times V(\lambda) \times V(\mu)$, let next $H_{\kappa,\lambda,\mu}$ and $L_{\kappa,\lambda,\mu}$ be permutation matrices satisfying

$$(22) \quad H^{-1}_{\kappa,\lambda,\mu} \begin{pmatrix} V(\kappa) \times V(\omega(\lambda,\mu)) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ V(\omega(\lambda,\mu)) \end{pmatrix} H_{\kappa,\lambda,\mu} = \begin{pmatrix} V(\omega(\lambda,\mu)) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ V(\omega(\lambda,\mu)) \end{pmatrix},$$

$$(23) \quad L^{-1}_{\kappa,\lambda,\mu} \begin{pmatrix} V(\omega(\lambda,\mu)) \times V(\omega(\lambda,\mu)) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ V(\omega(\lambda,\mu)) \end{pmatrix} L_{\kappa,\lambda,\mu} = \begin{pmatrix} V(\omega(\lambda,\mu)) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ V(\omega(\lambda,\mu)) \end{pmatrix}.$$
Then

\[(24) \quad L_{\kappa,\lambda,\mu} \left( \begin{array}{c} P_{\kappa,\omega_1(\lambda,\mu)} \\ \vdots \end{array} \right) H_{\kappa,\lambda,\mu} (I_{\theta(\kappa)} \times P_{\lambda,\mu}) = Q_{\kappa,\lambda,\mu} \left( \begin{array}{c} P_{\omega_1(\kappa,\lambda,\mu)} \\ \vdots \end{array} \right) (P_{\kappa,\lambda} \times I_{\theta(\mu)}) \]

with a non-singular matrix \( Q_{\kappa,\lambda,\mu} \) commutative with the representation \( \mathbb{V}^{(\omega_1(\kappa,\lambda,\mu))} \). There is matrix \( R_{\kappa,\lambda,\mu} \) such as

\[(25) \quad Q_{\kappa,\lambda,\mu}^{-1} \left( \begin{array}{c} \mathbb{F}^{(\omega_1(\kappa,\lambda,\mu))} \\ \vdots \end{array} \right) = \left( \begin{array}{c} \mathbb{F}^{(\omega_1(\kappa,\lambda,\mu))} \\ \vdots \end{array} \right) R_{\kappa,\lambda,\mu}. \]

These matrices \( H_{\kappa,\lambda,\mu}, L_{\kappa,\lambda,\mu}, Q_{\kappa,\lambda,\mu} \) and \( R_{\kappa,\lambda,\mu} \) are all determined by \( G \) (and \( \Omega \)) only. Calculating \( (\mathbb{F}^{(\kappa)} \times \mathbb{F}^{(\lambda)}) \times \mathbb{F}^{(\mu)} \) and \( \mathbb{F}^{(\kappa)} \times (\mathbb{F}^{(\lambda)} \times \mathbb{F}^{(\mu)}) \), we find that

\[(26) \quad \left( \begin{array}{c} P_{\omega_1(\kappa,\lambda,\mu)} \\ \vdots \end{array} \right) \left( \begin{array}{c} B_{\omega_1(\kappa,\lambda,\mu)} \\ \vdots \end{array} \right) (P_{\kappa,\lambda} \times I_{\theta(\mu)})(B_{\kappa,\lambda} \times I_{\theta(\mu)}) = R_{\kappa,\lambda,\mu} L_{\kappa,\lambda,\mu} \left( \begin{array}{c} P_{\omega_1(\kappa,\lambda,\mu)} \\ \vdots \end{array} \right) \left( \begin{array}{c} B_{\omega_1(\kappa,\lambda,\mu)} \\ \vdots \end{array} \right) H_{\kappa,\lambda,\mu} (I_{\theta(\kappa)} \times P_{\lambda,\mu})(I_{\theta(\lambda)} \times B_{\lambda,\mu}) \]

is necessary and sufficient for the associativity of \( \mathbb{V} \); the condition may be seen again as being in terms of \( \langle A_{\kappa,\lambda} \rangle \).

Finally, since the system \( \{A_{\kappa,\lambda}\} \) gives, by (17), the multiplication table of \( \mathbb{V} \), the regular discriminant of \( \mathbb{V} \) can be expressed by means of \( \{A_{\kappa,\lambda}\} \). Provided \( \mathbb{V} \) is associative (that is, (26) holds) its non-vanishing is necessary and sufficient in order that \( \mathbb{V} \) be absolutely semisimple and its capacities be all indivisible by the characteristic of \( \Omega \). However, on assuming both the commutativity and associativity we can obtain a second expression for the discriminant (whose non-vanishing is now necessary and sufficient for the absolute semisimplicity of \( \mathbb{V} \)) as follows. Namely, the trace of an element of \( \mathbb{V} \) may then be given as the sum of its transforms by \( G \). So the matrix composed of the traces of elements of \( \mathbb{F}^{(\kappa)} \times \mathbb{F}^{(\lambda)} \) is given by

\[(27) \quad \sum_{\mathbb{V}^{(\kappa)}} (\mathbb{F}^{(\kappa)} \times \mathbb{F}^{(\lambda)}) z = \sum_{z} (P_{\kappa,\lambda}^{-1})^{\ast} \left( \begin{array}{c} \mathbb{F}^{(\omega_1(\kappa,\lambda,\mu))} \\ \vdots \end{array} \right) P_{\kappa,\lambda} A_{\kappa,\lambda} z. \]

Making use of the orthogonality relation (15) we find that this is equal to

\[(28) \quad P_{\kappa,\lambda}^{-1} G'_{\kappa,\lambda} \left( \begin{array}{c} S^{(1)} \\ \vdots \end{array} \right) \left( \begin{array}{c} K^{(1)} \end{array} \right) \left( \begin{array}{c} (I_k \times 0) \\ \vdots \end{array} \right) \left( \begin{array}{c} K^{(1)} \\ \vdots \end{array} \right) G_{\kappa,\lambda} P_{\kappa,\lambda} A_{\kappa,\lambda} \]

multiplied by \( \gamma \) and the trace of \( \mathbb{I} \) (which is not 0). Now the part of our dis-
criminant matrix corresponding to the products of the basis elements from $U^{(\kappa)}$ and $\mathcal{U}^{(\lambda)}$ can be obtained from (28) by virtue of a certain, easily describable rearrangement of elements (except a non-zero scalar factor independent of $\kappa, \lambda$).

These together offer criterion for the associativity, commutativity and absolute semisimplicity of the Galois algebra $\mathcal{V}$ given by $\{A_{\kappa, \lambda}\}$.  

**References**


