On Galois modules of vector spaces.

By E. FRIED (Budapest).

§ 1. Introduction.

Let L be a finite algebraic extension of the field K and G the corresponding Galois group. The group algebra Γ of G with coefficients in K is called the Galois module of the extension $L|K$. Γ can also be considered as a ring of K-endomorphisms of the vector space L over K.[1] The extension $L|K$ can be discussed by the aid of the Galois module Γ rather than the Galois group G.

Several generalizations of the notion of Galois group are known. In a general case R. BAER [1] defined the Galois group for an arbitrary vector space L of finite dimension over a field, and proved that there exists a Galois correspondence between the subgroups of the Galois group and the corresponding subspaces of L.

Here we generalize the concept of Galois module Γ to arbitrary vector spaces L of finite dimension over a field K, with the intention of obtaining a general Galois correspondence between the right ideals of Γ and the annihilated subspaces of L.[2] Then a vector space of dimension >1 will have several non-isomorphic Galois modules over the same underlying field and the complete endomorphism ring will be only one of the possible Galois modules. The main result of this paper generalizes the so-called „normal basis" theorem. As a by-product we obtain a new proof of the normal basis theorem.[3]

[1] Γ is not the complete ring of endomorphisms unless $L=K$.

[2] Let L be a vector space over the field K and Γ a ring of operators acting on L such that the multiplications by the elements of K commute with the operators in Γ, i. e. for arbitrary $\lambda \in K, u \in L$ and $\eta \in \Gamma$ we have $(\lambda u)\eta = \lambda(u\eta)$. (We write the operators on the right.)

[3] M. DEURING used Galois modules in the proof of the normal basis theorem, but he made use of representation theory as well. (See [2].)

§ 2. Preliminaries.

Let K be a field, L a vector space over K and Γ a ring of K-endomorphisms of L. We define $X[Y]$ as follows:

case (a): if $X \subseteq L$ and $Y \subseteq \Gamma$, then let $X[Y]$ denote the set of all elements in X which are annihilated by every element of Y;

case (b): if $X \subseteq \Gamma$ and $Y \subseteq L$, then let $X[Y]$ denote the set of all elements in X which annihilate every element of Y.

For $L = \Gamma$ we define $X[Y]$ as in case (a).

It is obvious that $Y_1 \subseteq Y_2$ implies

(i) $$X[Y_1] \supseteq X[Y_2],$$

(ii) $$Y_2[X[Y_1]] \supseteq Y_1,$$

(iii) $$Y_2[X] \supseteq Y_1[X]$$

for arbitrary Y_1, Y_2 and X in L or in Γ.

Let L be a vector space of finite dimension over K and Γ a ring of K-endomorphisms of L. We speak about a *Galois correspondence* or *Galois connection* between L and Γ if the two lattices:

(a) the lattice $\mathfrak{L}(\Gamma)$ of right ideals J of Γ;

(b) the lattice $\mathfrak{L}_\Gamma(L)$ of the subspaces $L(J)$ of L annihilated by right ideals of Γ[4])

are anti-isomorphic.

Let M be the complete ring of K-endomorphisms of L and Δ a subspace of L. Clearly, $M[\Delta]$ is a right ideal of M. The correspondence $\Delta \to M[\Delta]$ is evidently a Galois correspondence between the subspaces Δ of L and the right ideals $M[\Delta]$ of M. Let $d(X)$ denote the dimension of the vector space X over K. It is easy to see that

(iv) $$d_L(\Delta) + d_M(M[\Delta]) = 1$$

for every subspace Δ of L where $d_Y(X) = d(X)/d(Y)$ for a subspace X of the vector space Y.

§ 3. Galois modules of a vector space.

Let K be a field and L a vector space of finite dimension over K. A subring Γ of the complete endomorphism ring M of L is called a *Galois module* of L if Γ is a vector space over K, $\Gamma M = M$ and for the right ideals J $(J \neq 0)$ of Γ

(v) $$d(JM)/d(J) \text{ is independent of } J.$$

(Here JM is the right ideal of M generated by J.)

[4]) That these subspaces form in fact a lattice will be shown in the proof of Theorem 1.

Γ being a right ideal of itself, we have $d(JM)/d(J)=d(\Gamma M)/d(\Gamma)=$ $=d(M)/d(\Gamma)$, that is, $d_M(JM)=d_\Gamma(J)$.

Let K be a field, L a vector space of finite dimension over K and Γ a Galois module of L. Then we have

Theorem 1. *The correspondence $J\to L[J]$ is a Galois connection between L and Γ, and*

$$d_\Gamma(J)+d_L(L[J])=1.$$

Proof. Let J be an arbitrary element of $\mathfrak{L}(\Gamma)$. The right ideals J and JM have the same basis, therefore $L[J]=L[JM]$. From (iv) and the Galois correspondence between the right ideals of M and the subspaces of L we obtain $1-d_\Gamma(J)-d_L(L[J])=1-d_\Gamma(J)-d_L(L[JM])=d_M(JM)-d_\Gamma(J)=0$, i. e.

(vi) $$d_\Gamma(J)+d_L(L[J])=1.$$

Let Δ be a subspace of L and J a right ideal of Γ. Applying (ii) with $Y_2=L$, $Y_1=\Delta$, $X=\Gamma$, and then with $Y_2=\Gamma$, $Y_1=J$, $X=L$, we obtain

(vii) $$L[\Gamma[\Delta]]\supseteq\Delta,$$

(viii) $$\Gamma[L[J]]\supseteq J,$$

respectively. (vi) and (vii) imply

(ix) $$d_L(\Delta)+d_\Gamma(\Gamma[\Delta])\leqq 1.$$

Putting $\Delta=L[J]$, from (viii), (ix) and (vi) we obtain the inequalities $d_\Gamma(J)\leqq d_\Gamma(\Gamma[L[J]])\leqq 1-d_L(L[J])=d_\Gamma(J)$. It follows that $d_\Gamma(J)=$ $=d_\Gamma(\Gamma[L[J]])$, and therefore by (viii) we have

(x) $$J=\Gamma[L[J]].$$

On the other hand, using the fact that $d_\Gamma(\Gamma[L[J]])=1-d_L(L[J])$, we obtain $d_\Gamma(\Gamma[\Delta])+d_L(\Delta)=1$ for $\Delta=L[J]$. From (x) we conclude that $L[J]=L[\Gamma[L[J]]]$, and therefore we obtain the equality $\Delta=L[\Gamma[\Delta]]$ for $\Delta=L[J]$.

Consequently, the correspondence $J\to L[J]$ is one-to-one between the right ideals J of Γ and the annihilated subspaces $\Delta=L[J]$ of L, and the formula $d_\Gamma(J)+d_L(L[J])=1$ holds.

It remains to prove that the correspondence is an anti-isomorphism.

If $\eta\in\Gamma[\Delta_1]\cap\Gamma[\Delta_2]$ and $u\in\Delta_1\cup\Delta_2$, then write u in the form $u=u_1+u_2$ $(u_i\in\Delta_i)$. We obtain $u\eta=u_1\eta+u_2\eta=0$, that is to say,

(xi) $$\Gamma[\Delta_1]\cap\Gamma[\Delta_2]\subseteq\Gamma[\Delta_1\cup\Delta_2].$$

If $u\in L[J_1]\cap L[J_2]$ and $\eta\in J_1\cup J_2$, then writing η in the form $\eta=\eta_1+\eta_2(\eta_i\in J_i)$, we obtain $u\eta=u\eta_1+u\eta_2=0$, i. e.

(xii) $$L[J_1]\cap L[J_2]\subseteq L[J_1\cup J_2].$$

On the other hand, owing to (i) we have $\Gamma[\Delta_1\cup\Delta_2]\subseteq\Gamma[\Delta_i]$, whence

(xiii) $$\Gamma[\Delta_1\cup\Delta_2]\subseteq\Gamma[\Delta_1]\cap\Gamma[\Delta_2],$$

and similarly

(xiv) $$L[J_1\cup J_2]\subseteq L[J_1]\cap L[J_2].$$

Comparing (xi) and (xiii), (xii) and (xiv), we obtain

(xv) $$\Gamma[\Delta_1\cup\Delta_2]=\Gamma[\Delta_1]\cap\Gamma[\Delta_2]$$

and

(xvi) $$L[J_1\cup J_2]=L[J_1]\cap L[J_2]$$

respectively. Substituting $L[J_i]$ for Δ_i in (xv) and $\Gamma[\Delta_i]$ for J_i in (xvi), we get

$$L[J_1\cap J_2]=L[\Gamma[L[J_1]]\cap\Gamma[L[J_2]]]=L[\Gamma[L[J_1]\cup L[J_2]]]\supseteq L[J_1]\cup L[J_2]$$

and

$$\Gamma[\Delta_1\cap\Delta_2]=\Gamma[L[\Gamma[\Delta_1]]\cap L[\Gamma[\Delta_2]]]=\Gamma[L[\Gamma[\Delta_1]\cup\Gamma[\Delta_2]]]=\Gamma[\Delta_1]\cup\Gamma[\Delta_2].$$

Next we prove that the vector spaces $L[J_1\cap J_2]$ and $L[J_1]\cup L[J_2]$ have the same dimension. Clearly, $d(\Delta_1\cap\Delta_2)+d(\Delta_1\cup\Delta_2)=d(\Delta_1)+d(\Delta_2)$ for arbitrary subspaces Δ_1,Δ_2 of L, and therefore

$$d_L(L[J_1]\cup L[J_2])=d_L(L[J_1])+d_L(L[J_2])-d_L(L[J_1]\cap L[J_2])=1-d_\Gamma(J_1)+$$
$$+1-d_\Gamma(J_2)-1+d_\Gamma(J_1\cup J_2)=1-d_\Gamma(J_1\cap J_2)=d_L(L[J_1\cap J_2]).$$

Consequently,

(xvii) $$L[J_1\cap J_2]=L[J_1]\cup L[J_2].$$

This completes the proof of Theorem 1.

REMARK. *Let Γ be a ring of endomorphisms of the vector space L. If $d_{\Gamma}(J)+d_\Gamma(L[J])=1$ for every right ideal J of Γ then Γ is a Galois module of L.* Indeed, using again $L[J]=L[JM]$ and (iv), we obtain $d_M(JM)=$ $=1-d_L(L[JM])=1-d_L(L[J])=d_\Gamma(J)$. Thus the number $d(JM)/d(J)=$ $=d(M)/d(\Gamma)$ is independent of J. In case $J=\Gamma$ we have $d(\Gamma M)/d(\Gamma)=$ $=d(M)/d(\Gamma)$, and therefore $\Gamma M=M$, q. e. d.

Theorem 2. *Let Γ be a Galois module of the vector space L, and J an arbitrary right ideal of Γ. J is a Galois module of the factor module $L/L[J]$ if every right ideal J' of J satisfies $J'=J'J$. In this case $d(\Gamma)/d(L)=$ $=d(J)/d(L/L[J])$.*

PROOF. It is obvious that J is a ring of endomorphisms of $L/L[J]$. By hypothesis, $J'\Gamma=J'J\Gamma\subseteq J'J=J'$, i. e. every right ideal J' of J is a right ideal of Γ. We have $d(J)/d(\Gamma)=(d(L)-d(L[J]))/d(L)$ and we know that $d(J')/d(\Gamma)=(d(L)-d(L[J']))/d(L)$ holds too. Hence

$$\frac{d(J')}{d(J)}+\frac{d(L[J']-d(L[J])}{d(L)-d(L[J])}=1 \text{ or } d_J(J')+d_{L/L[J']}((L/L[J])[J'])=1.$$

Because of the Remark above, J is a Galois module of $L/L[J]$ and, clearly, $d(\Gamma)/d(L)=d(J)/d(L/L[J])$.

Theorem 3. *Let Γ be a Galois module of the vector space L and $I\ (\neq \Gamma)$ an arbitrary ideal of Γ. Then Γ/I is a Galois module of $L[I]$ and $d(\Gamma)/d(L)=$ $=d(\Gamma/I)/d(L[I])$.*

PROOF. It is obvious that Γ/I is an endomorphism ring of $L[I]$. Every right ideal of Γ/I has the form J/I where $J(\supseteq I)$ is a right ideal of Γ. Therefore $d(L[I])/d(L)=(d(\Gamma)-d(I))/d(\Gamma)$ and $d(L[J])/d(L)=(d(\Gamma)-d(J))/d(\Gamma)$. By division we get

$$\frac{d(L[J])}{d(L[I])}+\frac{d(J)-d(I)}{d(\Gamma)-d(I)}=1 \text{ or } d_{L[I]}((L[I])[J/I])+d_{\Gamma/I}(J/I)=1$$

whence Theorem 3 follows by making use of our Remark. The proof of $d(\Gamma)/d(L)=d(\Gamma/I)d(L[I])$ is clear.

In a definite case it is not easy decide whether or not (v) holds for a subring Γ of the complete ring of endomorphisms M. Now we proceed to an important class of Galois modules of L for which the fulfilment of (v) is easier to decide.

Let us consider an algebra C over some field K and two subalgebras A and B of C. Suppose $C=AB$, where AB denotes the product algebra (which consists of all finite sums $\Sigma a_i b_i\ (a_i\in A, b_i\in B)$). Let $\alpha_1,\dots,\alpha_n,\dots$ and $\beta_1,\dots,\beta_k,\dots$ be bases of A and B, respectively. Let us define the set $\dots,\alpha_i\beta_j,\dots$ as the product of the bases $\alpha_1,\dots,\alpha_n,\dots$ and $\beta_1,\dots,\beta_k,\dots$. The algebra C is called the semi-direct product of its subalgebras A and B, if there exist bases $\alpha_1,\dots,\alpha_n,\dots$ of A and $\beta_1,\dots,\beta_k,\dots$ of B such that their product is a basis of C. In this case C is denoted by $A(\times)B$. It is obvious that if $C=A(\times)B$, then the product of any bases of A and B is a basis of C. It is also evident that in the finite case $C=A(\times)B$ holds if and only if $d(C)=d(A)\cdot d(B)$. In general, $A(\times)B\neq B(\times)A$, and it is easy to see that $A(\times)B=B(\times)A$ does not imply that $C=A\times B$, the direct product of A and B.

Theorem 4. *Let K be a field, L a vector space of finite dimension over K, and M the complete ring of endomorphisms of L. If there exist subalgebras Γ and Γ' of M such that $M=\Gamma(\times)\Gamma'$, then Γ is a Galois module of L.*

PROOF. Γ is obviously a ring of endomorphisms of L. We have to prove that (v) holds for Γ. Because of $\Gamma M\supseteq\Gamma\Gamma'=M\supseteq\Gamma M$ we get $\Gamma M=M$. If J is a right ideal of Γ, then our hypothesis implies that the product $J\Gamma'$ is semi-direct. Thus $JM=J(\Gamma(\times)\Gamma')=J(\times)\Gamma'$, i. e. $d(JM)=d(J)\cdot d(\Gamma')$, q. e. d.

§ 4. Galois modules operator-isomorphic to the vector space.

In this section we intend to prove a generalisation of the normal basis theorem. Let L be a finite separable and normal algebraic extension of the field K. The normal basis theorem asserts that there exists a basis of L over K which consists of all conjugates of an element of L. We shall prove that if we consider L as a vector space over K, then the group algebra Γ_K^G of the Galois group G of $L|K$ over K is a Galois module of L, further that the normal basis theorem is equivalent to the assertion that L contains an element which is not annihilated by any non-zero element of Γ_K^G. Hence we shall conclude that L and Γ_K^G are operator-isomorphic with respect to Γ_K^G as operator-domain.

Let L be a vector space of finite dimension over K, and Γ a Galois module of L. Suppose that $\Gamma \cong_\Gamma L$, i. e. Γ and L are Γ-isomorphic, and let φ be a fixed operator-isomorphism between Γ and L. Thus if $\eta \in \Gamma$ and $\varphi(\eta) \in L$, then $\varphi(\eta\xi) = \varphi(\eta)\xi$ for all $\xi \in \Gamma$, and therefore $\varphi(\eta)\xi = 0$ if and only if $\eta\xi = 0$. Consequently, $\varphi(\eta) \in L[J]$ if and only if $\eta \in \Gamma[J]$. Hence the operator-isomorphism implies $d(\Gamma) = d(L)$ and $d(\Gamma[J]) = d(L[J])$. From the hypotheses we conclude that $d(\Gamma[J]) + d(J) = d(\Gamma)$. It is easy to see that $\Gamma[J]$ is a left ideal of Γ. Γ being an endomorphism ring of itself, from what has been said it results:

Theorem 5. *If Γ is a Galois module of L which is Γ-isomorphic to L, then Γ is a Galois module of itself, further, for every right ideal J of Γ, $\Gamma[J]$ is a left ideal and $d(J) + d(\Gamma[J]) = d(\Gamma)$ holds.*

Before turning to the proof of the converse assertion, we consider some needed lemmas.

LEMMA 1. *Every simple, non-nilpotent algebra Γ of finite rank over a field K is a Galois module of itself.*

Every right ideal of Γ may be written in the form $\varepsilon\Gamma$ with an idempotent ε. If 1 denotes the identity of Γ, then evidently $\Gamma[\varepsilon\Gamma] = \Gamma(1-\varepsilon)$ whence $d(\Gamma[\varepsilon\Gamma]) = d(\Gamma(1-\varepsilon)) = d((1-\varepsilon)\Gamma) = d(\Gamma) - d(\varepsilon\Gamma)$.

LEMMA 2. *Every semi-simple algebra Γ over a field K is a Galois module of itself.*

By Lemma 1 this is true if Γ is simple. By a known theorem, Γ is the direct sum of a finite number of simple algebras, say, of k simple algebras. Assume that the lemma has been proved for semi-simple algebras which are direct sums of at most $k-1$ simple algebras. If Γ is not simple, then write Γ as a direct sum

$$\Gamma = \Gamma_1 + \Gamma_2,$$

where Γ_1, Γ_2 are non-zero subalgebras of Γ. Γ_i is a Galois module of itself by the inductive assumption. Let J be a right ideal of Γ. Because Γ contains an identity, we have $J = J_1 + J_2$. By direct sum property, we infer $\Gamma[J] = \Gamma[J_1] \cap \Gamma[J_2]$. On the one hand we have $\Gamma[J_1] = \Gamma_1[J_1] + \Gamma_2$, and on the other hand $\Gamma[J_2] = \Gamma_1 + \Gamma_2[J_2]$. Therefore $\Gamma[J] = \Gamma[J_1] \cap \Gamma[J_2] = \Gamma_1[J_1] + \Gamma_2[J_2]$ whence $d(\Gamma[J]) + d(J) = d(\Gamma_1[J_1]) + d(\Gamma_2[J_2]) + d(J_1) + d(J_2) = d(\Gamma_1) + d(\Gamma_2) = d(\Gamma)$.

Theorem 6. *Let Γ be an algebra of finite rank over K, and suppose that Γ is a Galois module of itself. If Γ is Galois module of the vector space L of finite dimension over K and $d(\Gamma) = d(L)$, then there exists an element in L which is not annihilated by any element of Γ different from zero.*

PROOF. *Case I: Γ is simple and not nilpotent.* It is known that in this case Γ may be written in the form

$$\text{(xviii)} \qquad \Gamma = F \times P_r,$$

where F is a skew-field over K and P_r is a complete matrix ring of finite order r over K. Let $\alpha_1, \dots, \alpha_s$ be a basis of F over K and $0 \neq u \in L$. If $\sum_{i=1}^{s} \lambda_i(u\alpha_i) = 0$ $(\lambda_i \in K)$, then $u\left(\sum_{i=1}^{s} \lambda_i \alpha_i\right) = 0$. Since $\sum_{i=1}^{s} \lambda_i \alpha_i \in F$ cannot have an inverse (otherwise we should have $u = 0$), we obtain $\sum_{i=1}^{s} \lambda_i \alpha_i = 0$, hence $\lambda_i = 0$ and the elements $u\alpha_1, \dots, u\alpha_s$ are linearly independent. Therefore L as a right vector space over F is of dimension r^2. Choose elements $\dots, \varepsilon_{ij}, \dots$ of P_r such that $\varepsilon_{ij}\varepsilon_{kl} = \delta_{jk}\varepsilon_{il}$ where δ_{jk} is the Kronecker symbol $(1 \leqq i, j, k, l \leqq r)$. Then the elements $\varepsilon_i = \varepsilon_{ii}$ are primitive orthogonal idempotents and $\varepsilon_1 + \dots + \varepsilon_r = 1$ is the identity of Γ. By (xviii), $L\varepsilon_1$ is a right vector space over F. It is obvious that $L = L\varepsilon_1 + L(1-\varepsilon_1)$ and $L[\varepsilon_1\Gamma] = L(1-\varepsilon_1)$. Thus $d(L\varepsilon_1) = d(L) - d(L(1-\varepsilon_1)) = d(\Gamma) - d(L[\varepsilon_1\Gamma]) = d(\varepsilon_1\Gamma) = d(F)\cdot r$, i. e. the dimension of $L\varepsilon_1$ over F is exactly r. Let $u_1, \dots, u_r$ be a basis of $L\varepsilon_1$ over F, and consider the elements

$$\text{(xix)} \qquad u_{ij} = u_i\varepsilon_{1j} \qquad (1 \leqq i, j \leqq r).$$

If $\sum_{i,j} u_{ij}\alpha_{ij} = 0$ for the elements α_{ij} of F, then $0 = 0 \cdot \varepsilon_{k1} = \sum_{i,j} u_{ij}\alpha_{ij}\varepsilon_{k1} = \sum_{i,j} u_i\varepsilon_{1j}\alpha_{ij}\varepsilon_{k1} = \sum_i u_i\alpha_{ik}$. We infer $\alpha_{ik} = 0$ $(1 \leqq i, k \leqq r)$. By the basis property of the u_i, the elements in (xix) form a basis of L over F. Let us consider now the element $u = \sum_{i=1}^{r} u_{ii} \in L$. Suppose that $u\eta = 0$ for some element

$\eta = \sum_{j,k} \varepsilon_{jk}\alpha_{jk}$ of Γ $(\varepsilon_{jk} \in P_r, \alpha_{jk} \in F, 1 \leqq j, k \leqq r)$. Owing to $u_{ij}\varepsilon_{kl} = u_i \varepsilon_{1j}\varepsilon_{kl} = \delta_{jk} u_i \varepsilon_{1l} = \delta_{jk} u_{il}$ we obtain $0 = \sum_i u_{ii} \sum_{j,k} \varepsilon_{jk}\alpha_{jk} = \sum_{i,j,k} u_{ii}\varepsilon_{jk}\alpha_{jk} = \sum_{i,k} u_{ik}\alpha_{ik}$. Since the elements in (xix) form a basis over F, it follows that $\alpha_{ik} = 0$, $\eta = 0$. Consequently, u has the required property.

Case II: Γ is semi-simple. As in the proof of Lemma 2, we write Γ as a direct sum $\Gamma = \Gamma_1 + \Gamma_2$ $(\Gamma_t \neq 0)$. By Theorem 3 and by $\Gamma_1 \cong \Gamma/\Gamma_2$, $\Gamma_2 \cong \Gamma/\Gamma_1$, Γ_1 and Γ_2 are Galois modules of $L[\Gamma_2]$ and $L[\Gamma_1]$, respectively, and we have $d(\Gamma_1) = d(L[\Gamma_2])$, $d[\Gamma_2] = d(L[\Gamma_1])$. From (xvi) and (xvii) we obtain $0 = L[\Gamma] = L[\Gamma_1 \cup \Gamma_2] = L[\Gamma_1] \cap L[\Gamma_2]$ and $L = L[0] = L[\Gamma_1 \cap \Gamma_2] = L[\Gamma_1] \cup L[\Gamma_2]$. Thus putting $L_1 = L[\Gamma_2]$ and $L_2 = L[\Gamma_1]$ we get

$$L = L_1 + L_2 \tag{xx}$$

where Γ_t is a Galois module of L_t and $d(L_t) = d(\Gamma_t)$ $(t = 1, 2)$.

By an obvious inductive hypothesis, we may assume that there exists an element u_t of L_t such that u_t is not annihilated by any non-zero element of Γ_t different from 0 $(t = 1, 2)$. Assume that for $u = u_1 + u_2$ $(u_t \in L_t)$ and for some element η of Γ, $\eta = \eta_1 + \eta_2$ $(\eta_t \in \Gamma_t)$, we have $u\eta = 0$. Then $0 = u\eta = u_1\eta_1 + u_2\eta_2$ and the directness of (xx) implies $u_t\eta_t = 0$, whence $\eta_t = 0$ and $\eta = 0$. Thus u is an adequate element of L.

Case III: Γ is arbitrary. Let R denote the radical of Γ and put $D = L[R]$. By Theorem 3, Γ/R is a Galois module of D and we have $d(\Gamma/R) = d(D)$. Γ/R being semi-simple, by Lemma 2 and case II there exists in D an element u annihilated by no element of Γ/R different from 0. For this element u we have $d(u \cdot \Gamma/R) = d(\Gamma/R) = d(D)$ and thus $D = u \cdot \Gamma/R$. But $D = L[R]$, so that also $D = u\Gamma$. Putting $I = \Gamma[R]$ and applying this result to L instead of Γ, we obtain that I has an element ξ such that $I = \xi\Gamma$. Then $L\xi \subseteq D$ since $\xi \in \Gamma[R]$. Now $\xi \in I$ implies $L[I] \subseteq L[\xi]$, consequently, $L[I] = L[\xi]$. For an endomorphism, the sum of the dimensions of the kernel and the image is equal to the dimension of the vector space, therefore $d(L\xi) = d(L) - d(L[I]) = d(\Gamma) - d(R) = d(D)$, because of $d(L[I]) + d(I) = d(\Gamma)$ and $d(R) + d(I) = d(\Gamma)$, i. e. $L\xi = D$. Hence there exists a $v \in L$ such that $v\xi = u$. Any element of I may be written in the form $\xi\eta$ $(\eta \in \Gamma)$. If $v(\xi\eta) = 0$, then $0 = v(\xi\eta) = u\eta$, and so $\eta \in R$, $\xi\eta = 0$. Thus 0 is the only element of I annihilating v.

Let $J \neq 0$ be a right ideal of Γ. R being nilpotent, there exists a non-negative integer n such that $JR^n \neq 0$ and $(JR^n)R = JR^{n+1} = 0$. For this n we have clearly

$$0 \neq JR^n \subseteq J \cap \Gamma[R] = J \cap I. \tag{xxi}$$

In the preceding paragraph we have proved that the intersection of I and the right ideal J annihilating v is 0. Therefore (xxi) implies $J=0$, completing the proof of Theorem 6.

Let now u be an element of L whose existence is stated in Theorem 6. If $\eta_1, \dots, \eta_n$ is a basis of Γ then, clearly, $u\eta_1, \dots, u\eta_n$ is a basis of L. Thus every element of L may be written in the form $u\eta (\eta \in \Gamma)$. It follows readily that the mapping $\eta \rightarrow u\eta$ is an operator-isomorphism between Γ and L. This proves

Theorem 7. *Let Γ be an algebra of finite dimension over K, and suppose that Γ is a Galois module of itself. If Γ is a Galois module of the vector space L of finite dimension over K and $d(\Gamma)=d(L)$ then $\Gamma \cong_\Gamma L$.*

Let us mention the following fact. Since every element of L has the form $u\eta (\eta \in \Gamma)$, there exists an $\varepsilon \in \Gamma$ such that $u = u\varepsilon$. Then for any $\eta \in \Gamma$, we have $u\eta = (u\varepsilon)\eta = u(\varepsilon\eta)$, i. e. $u(\eta - \varepsilon\eta) = 0$, whence $\eta = \varepsilon\eta$, ε is a left identity of Γ. Because of $(\eta - \eta\varepsilon)\xi = (\eta - \eta\varepsilon)\varepsilon\xi = (\eta\varepsilon - \eta\varepsilon)\xi = 0$ $(\eta, \xi \in \Gamma)$ it follows that $\eta - \eta\varepsilon \in \Gamma[\Gamma] = 0$, $\eta = \eta\varepsilon$, and we arrive at

Theorem 8. *If the algebra Γ of finite rank over K is a Galois module of itself, then Γ has an identity.*

We turn to derive the consequences of Theorem 6 for algebraic extension fields.

First let us consider an arbitrary group G and a field K. The group algebra Γ_K^G of G over K consists of all finite sums of the form $\sum_i \lambda_i \sigma_i$ $(\lambda_i \in K, \sigma_i \in G)$. The elements of the group G form a basis of Γ_K^G and the product of two basis elements is the same as their product in G.

Theorem 9. *For finite groups G the group algebra $\Gamma = \Gamma_K^G$ is a Galois module of itself.*

Let M be the complete endomorphism ring of Γ, and $\varepsilon_j \in M$ such that $\sigma_i \varepsilon_j = \delta_{ij} \sigma_i$ $(1 \leqq i, j \leqq d(\Gamma) = n = \text{order of } G)$. Consequently, $\varepsilon_j \varepsilon_k = 0, \varepsilon_j^2 = \varepsilon_j$ $(1 \leqq j \neq k \leqq n)$, the ε_j are orthogonal idempotents, and $\sum_{j=1}^{n} \varepsilon_j = 1$ is the identity of M. It is easy to verify that the subspace D of M generated by the elements ε_j is an algebra over K. Since $d(D) = d(\Gamma)$, the elements ε_j are primitive idempotents.

Denote by $\bar{\sigma}_i$ the right multiplication by σ_i; this is an endomorphism of Γ and the $\bar{\sigma}_i$ $(1 \leqq i \leqq n)$ span in M a subalgebra $\bar{\Gamma}$ isomorphic to Γ, an isomorphism being induced by $\sigma_i \rightarrow \bar{\sigma}_i$. We intend to show that the elements $\bar{\sigma}_i \varepsilon_j$ $(1 \leqq i, j \leqq n)$ form a basis of M over K. Suppose $\eta = \sum_{i,j} \lambda_{ij} \bar{\sigma}_i \varepsilon_j = 0$ $(\lambda_{ij} \in K)$; then η belongs to $\bar{\Gamma} D \subseteq M$. In order to verify $\lambda_{pq} = 0$ for some fixed indices p, q, consider $0=(\sigma_q\sigma_p^{-1})\eta=\sum_{i,j}\lambda_{ij}(\sigma_q\sigma_p^{-1})\bar{\sigma}_i\varepsilon_j=\sum_{i,j}\lambda_{ij}(\sigma_q\sigma_p^{-1}\sigma_i)\varepsilon_j$. This may be written as a linear combination of the σ_i; $(\sigma_q\sigma_p^{-1}\sigma_i)\varepsilon_j=\sigma_q$ if and only if $j=q$ and $i=p$, i. e. the coefficient of σ_q will be λ_{pq}. Because of the linear independence of the σ_i we obtain $\lambda_{pq}=0$, and thus the $\bar{\sigma}_i\varepsilon_j$ are linearly independent. Their number is equal to the dimension of M, whence $\bar{\Gamma}(\times)D=M$. Theorem 4 completes the proof.

Theorem 10. *Let L be a finite, separable and normal algebraic extension of the field K, and G the Galois group of this extension. If L is considered as a vector space over K, then $\Gamma=\Gamma_K^G$ is a Galois module of L.*

It is obvious that both L and Γ are endomorphism rings of L, and thus $\Gamma L\subseteq M$, where M is the complete endomorphism ring of L. An arbitrary element η of ΓL may be written in the form $\eta=\sum_{i=1}^{n}\sigma_i w_i (n=d(L), \sigma_i\in G, w_i\in L)$. Let v be a primitive element of the extension $L|K$. If every element of L is annihilated by $\eta\in\Gamma$, then $0=(v^k)\eta=\sum_{i=1}^{n}(v^k)\sigma_i w_i=\sum_{i=1}^{n}v_i^k w_i$ $(0\leqq k\leqq n-1)$ where $v_i=v\sigma_i$ are the conjugates of v. Consider the equations $\sum_{i=1}^{n}v_i^k w_i=0$ as a system of homogeneous linear equations with unknowns w_i whose determinant is of Vandermonde's type. This determinant is, because of separability, different from 0, therefore $w_i=0$ $(i=1,\dots,n)$ and $\eta=0$. Now in view of $d(\Gamma)=d(L)$ it follows that $M=\Gamma(\times)L$. Combining this with Theorem 4, the proof is completed.

Finally we prove

Theorem 11. *Every finite, separable and normal algebraic extension L of a field K has a normal basis.*

Owing to Theorems 6, 9 and 10, L contains an element u such that $u\eta=0$ $(\eta\in\Gamma_K^G)$ if and only if $\eta=0$. This means — writing $\eta\in\Gamma_K^G$ in the form $\eta=\sum\lambda_i\sigma_i$ with $\lambda_i\in K, \sigma_i\in G$ — that $\sum_{i=1}^{n}\lambda_i u_i=0$ if and only if $\lambda_i=0$ where $u_i=u\sigma_i$ are the conjugates of u. Thus the u_i $(i=1,\dots,n)$ form a basis of $L|K$, q e. d.

Bibliography.

[1] R. Baer, A Galois theory of linear systems over commutative fields, *Amer. J. Math.* **62** (1940), 551—558.

[2] M. Deuring, Galoissche Theorie und Darstellungstheorie, *Math. Ann.* **107** (1933), 140—144.

(Received November 26, 1958.)