ON SEMI-LINEAR NORMAL BASIS

By

Takesi ONODERA

§ 1. Introduction

As an extension of a normal basis theorem in Galois theory of fields T. Nakayama obtained the following so-called semi-linear normal basis theorem: Let L be a finite separable Galois extension field of a subfield K with the Galois group $\mathfrak{G}$, and let F be a subfield of L (not necessarily containing K) such that $F^{\mathfrak{G}} \subseteq F$. Then there exists in L an element whose $[L:K]$ conjugates with respect to L are linearly independent over F or form a generating system of L over F according as $[L:F] \geqq \text{or} \leqq [L:K]$. And he extended the theorem to the case of Galois extensions of division rings under some conditions [7, Assumptions I, II].

The main purpose of this paper is to extend the theorem to the case of strictly Galois extensions of division rings (Theorem 3).

On the other hand, F. Kasch considered in [5] the normal basis theorem in Noether's sense (Die zweite Fassung des Satz von der Normalbasis) for Galois extensions of division rings and obtained a necessary and sufficient condition under which the theorem holds [5, Satz 9]. His result will be easily generalized to the case of our semi-linear normal basis.

In §2, as a preliminary, we shall give a theorem on projective modules over a ring with minimum condition due to Nakayama and Nagao which serves as a main tool in our present considerations (Theorem 1). In §3, we shall give the proof of Theorem 3 and try to generalize some of Kasch's results. As an application of Theorem 1, we shall give in §4 a proof of a theorem on finite dimensional central division algebras due to Brauer and Albert.

§ 2. Preliminary results on projective modules over rings with minimum condition

Throughout this section, we assume that R is a ring with a unit element 1 and R satisfies the minimum condition for right ideals. As is well known R is decomposed into a direct sum of finite number of directly indecomposable right ideals e_iR, $i=1, \cdots, r$.

$$(1) \qquad R = \sum_{i=1}^{r} \oplus e_i R$$

where $E=\{e_i;\ i=1,\cdots,r\}$ is a set of primitive idempotent elements in R which are mutually orthogonal and such that $1=e_1+\cdots+e_r$.

Let N be the (nilpotent) radical of R. For an element a in R we denote by $\bar{a}$ the class determined by a in the semi-simple residue class ring $\bar{R}=R/N$. It is well known that an idempotent element e in R is primitive if and only if $\bar{e}$ is primitive in $\bar{R}$, and two primitive idempotent elements e and f in R are isomorphic (in the sense that the two right R-modules eR and fR are R-isomorphic) if and only if $\bar{e}$ and $\bar{f}$ are so in $\bar{R}$. From (1) we obtain the following decomposition of $\bar{R}$ into a direct sum of minimal right ideals:

$$(2) \qquad \bar{R} = \sum_{i=1}^{r} \oplus \bar{e}_i \bar{R}\,.$$

Here each $\bar{e}_i\bar{R}$ is an irreducible right R-module. Since $\bar{R}$ is semi-simple, every unital[1] irreducible right R-module ($\neq 0$) is $\bar{R}$-, whence R-isomorphic to some of $\bar{e}_i\bar{R}$.

Changing indices, we suppose that $\{e_1,\cdots,e_s\}$ is a complete set of all non-isomorphic idempotent elements in E and denote by $f(k)$ the number of idempotent elements in E which are isomorphic to e_k. Then we have R-isomorphisms:

$$(1)' \qquad R \cong \sum_{k=1}^{s} \oplus (e_k R)^{f(k)}$$

$$(2)' \qquad \bar{R} \cong \sum_{k=1}^{s} \oplus (\bar{e}_k \bar{R})^{f(k)}$$

where $(e_kR)^{f(k)}$ and $(\bar{e}_k\bar{R})^{f(k)}$ denote the direct sum of $f(k)$-copies of the right R-modules e_kR and $\bar{e}_k\bar{R}$ respectively.

Let $\mathfrak{M}$ be a right R-module. The following characterization of projective right R-modules was established by Nakayama and Nagao in [8], but for the sake of completeness, we shall give here a simplified proof.[2]

Theorem 1. *$\mathfrak{M}$ is R-projective if and only if it is R-isomorphic to a direct sum of finite or infinite number of submodules which are R-isomorphic to the right ideal components e_kR's of R;*

1) In the sequel all modules considered are supposed to be unital in the sense that the unit element of a ring operates as an identity operator on the modules.

2) Theorem 1 and the present proof of it was informed by Prof. Azumaya to me. The theorem remains valid, as Eilenberg pointed in [3], when $R \ni 1$ is a semi-primary ring with nilpotent radical, that is, a ring with nilpotent radical N such that the residue class ring R/N is a semi-simple ring with minimum condition.

$$\mathfrak{M} \cong \sum_{k=1}^{s}{}_{\oplus}(e_k R)^{\mu_k}$$

and when this is the case the numbers μ_k's are uniquely determined by $\mathfrak{M}$.

Before proving the theorem, we shall prove the following

Lemma 1. *Let $\mathfrak{M}$ be a right R-module and let $\mathfrak{N}$ be a submodule of $\mathfrak{M}$ such that $\mathfrak{M}=\mathfrak{N}+\mathfrak{M}N$. Then we have $\mathfrak{M}=\mathfrak{N}$.*

Proof. Let $N^{\rho}=0$. From the supposition we have $\mathfrak{M}N=\mathfrak{N}N+\mathfrak{M}N^2$, whence we have $\mathfrak{M}=\mathfrak{N}+\mathfrak{N}N+\mathfrak{M}N^2=\mathfrak{N}+\mathfrak{M}N^2$. Repeating this process, we have

$$\mathfrak{M}=\mathfrak{N}+\mathfrak{M}N=\mathfrak{N}+\mathfrak{M}N^2=\mathfrak{N}+\mathfrak{M}N^3=\cdots=\mathfrak{N}+\mathfrak{M}N^{\rho}=\mathfrak{N}\,.$$

This proves our lemma.

Proof of Theorem 1. Since every e_kR is R-projective, the sufficiency of the condition is obvious. To prove the converse, let $\mathfrak{M}$ be a projective R-module and consider the residue module $\overline{\mathfrak{M}}=\mathfrak{M}/\mathfrak{M}N$. $\overline{\mathfrak{M}}$ is naturally regarded as an $\bar{R}$-module, and since $\bar{R}$ is semi-simple $\overline{\mathfrak{M}}$ is a completely reducible $\bar{R}$-module. Hence there is an ($\bar{R}$- or)R-isomorphism φ;

$$\varphi:\ \overline{\mathfrak{M}} \cong \sum_{k=1}^{s}{}_{\oplus}(\bar{e}_k\bar{R})^{\mu_k}$$

where μ_k's are finite or infinite cardinal numbers. Setting $Q=\sum_{k=1}^{s}{}_{\oplus}(e_kR)^{\mu_k}$, we assert that Q is R-isomorphic to $\mathfrak{M}$.

Consider the following diagram of R-modules and R-homomorphisms with the exact row:

$$\begin{array}{ccccc} & & Q & & \\ & & \downarrow{\scriptstyle \nu} & & \\ \mathfrak{M} & \xrightarrow{\varphi_0\mu} & \bar{Q}=Q/QN & \longrightarrow & 0 \end{array}$$

where φ_0 denotes an R-isomorphism of $\overline{\mathfrak{M}}$ onto $\bar{Q}\left(\cong \sum_{k=1}^{s}{}_{\oplus}(\bar{e}_k\bar{R})^{\mu_k}\right)$ and ν, μ denote the natural R-homomorphisms of Q and $\mathfrak{M}$ onto $\bar{Q}$ and $\overline{\mathfrak{M}}$ respectively. Since Q is R-projective, there exists an R-homomorphism f of Q into $\mathfrak{M}$ such that $\varphi_0\mu f=\nu$. Noting that $\varphi_0\mu$ maps $f(Q)$ onto $\bar{Q}$ and $\mathfrak{M}N$ is the kernel of $\varphi_0\mu$, we have

$$\mathfrak{M}=f(Q)+\mathfrak{M}N\,.$$

Then by the above lemma we obtain $\mathfrak{M}=f(Q)$, that is, f maps Q onto $\mathfrak{M}$.

Since $\mathfrak{M}$ is R-projective, there exists an R-homomorphism g of $\mathfrak{M}$ into Q such that $fg=1_{\mathfrak{M}}$ (the identity mapping of $\mathfrak{M}$). It is ovbious that g is a 1–1 mapping of $\mathfrak{M}$ into Q.

Since $\nu g=\varphi_0\mu fg=\varphi_0\mu$, ν maps $g(\mathfrak{M})$ onto $\bar{Q}$ and hence we have

$$Q=g(\mathfrak{M})+QN.$$

Hence, again by the lemma, we get $Q=g(\mathfrak{M})$. Thus g is an R-isomorphism of $\mathfrak{M}$ onto Q, and this secures our assertion.

Since $\overline{\mathfrak{M}}=\mathfrak{M}/\mathfrak{M}N\cong\sum_{k=1}^{s}{}_{\oplus}(\bar{e}_k\bar{R})^{\mu_k}$, and $\bar{e}_i\bar{R}$ and $\bar{e}_j\bar{R}$ are not R-isomorphic if $i\neq j$, the uniqueness of μ_k's follows from the theory of completely reducible modules.

Corollary 1. *Let $\mathfrak{M}$ be a right R-module such that*

$$\mathfrak{M}^{(n)}\cong R^{(m)}$$

for positive integers n and m. If $m=nq+r$ $(0\leqq r<n)$, then we have an R-isomorphism

$$\mathfrak{M}\cong R^{(q)}\oplus\mathfrak{m}$$

where $\mathfrak{m}$ is an R-homomorphic image of the right R-module R such that $\mathfrak{m}^{(n)}\cong R^{(r)}$. Especially, if $n=m$ then $\mathfrak{M}$ and R are R-isomorphic, and if $m<n$ then $\mathfrak{M}$ is an R-homomorphic image of R.

Proof. From the supposition we see that $\mathfrak{M}$ is R-projective. Hence by Theorem 1 we have an R-isomorphism

$$\mathfrak{M}\cong\sum_{k=1}^{s}{}_{\oplus}(e_kR)^{g(k)}$$

where $g(k)$'s are finite or infinite cardinal numbers. This implies again by Theorem 1 that

$$g(k)n=f(k)m=f(k)nq+f(k)r, \qquad k=1,\cdots,n.$$

Thus we have $g(k)=f(k)q+t(k)$, $0\leqq t(k)=f(k)r/n<f(k)$, and so $\mathfrak{m}=\sum_{k=1}^{s}{}_{\oplus}(e_kR)^{t(k)}$ is the required module.

Corollary 2. *If*

$$\mathfrak{M}^{(n)}\cong R^{(\omega)}$$

for a positive integer n and an infinite cardinal number ω, then we have an R-isomorphism:

$$\mathfrak{M} \cong R^{(\omega)} .$$

Proof. As in the same way in the proof of Corollary 1, we have $g(k)n = f(k)\omega = \omega$. Hence we get $g(k) = \omega$, and this proves our assertion.

Theorem 2. *Let $\mathfrak{M}$ be a projective R-module and let $\mathfrak{N}$ be an R-module. If $\mathfrak{N}^{(n)}$ is R-isomorphic to $\mathfrak{M}^{(n)}$ where n denotes a positive integer, then $\mathfrak{N}$ is R-isomorphic to $\mathfrak{M}$. Moreover if $\mathfrak{N}^{(m)}$ is R-homomorphic to $\mathfrak{M}^{(n)}$ where n and m are positive integers such that $n \leqq m$, then $\mathfrak{N}$ is R-homomorphic to $\mathfrak{M}$.*

Proof. The first half of the theorem easily follows from Theorem 1. To prove the last half of the theorem, let φ be an R-homomorphism of $\mathfrak{M}^{(n)}$ onto $\mathfrak{N}^{(m)}$. Then φ induces an R-homomorphism of $\mathfrak{M}^{(n)}/\mathfrak{M}^{(n)}N = \mathfrak{M}^{(n)}/(\mathfrak{M}N)^{(n)}$ $(\cong (\mathfrak{M}/\mathfrak{M}N)^{(n)}$ onto $\mathfrak{N}^{(m)}/\mathfrak{N}^{(m)}N = \mathfrak{N}^{(m)}/(\mathfrak{N}N)^{(m)}$ $(\cong (\mathfrak{N}/\mathfrak{N}N)^{(m)})$. Then since $(\mathfrak{M}/\mathfrak{M}N)^{(n)}$ and $(\mathfrak{N}/\mathfrak{N}N)^{(m)}$ are completely reducible R-modules, as is easily seen from the theory of completely reducible modules, $\overline{\mathfrak{N}} = \mathfrak{N}/\mathfrak{N}N$ is itself an R-homomorphic image of $\overline{\mathfrak{M}} = \mathfrak{M}N$. Let φ_0 be an R-homomorphism of $\overline{\mathfrak{M}}$ onto $\overline{\mathfrak{N}}$ and consider the following diagram of R-modules and R-homomorphisms with the exact row:

$$\begin{array}{ccccc} \mathfrak{M} & & & & \\ \downarrow{\scriptstyle \mu} & & & & \\ \overline{\mathfrak{M}} & & & & \\ \downarrow{\scriptstyle \varphi_0} & & & & \\ \mathfrak{N} & \xrightarrow{\nu} & \overline{\mathfrak{N}} & \longrightarrow & 0 \end{array}$$

where μ, ν denote the natural mappings of $\mathfrak{M}$ and $\mathfrak{N}$ onto $\overline{\mathfrak{M}}$ and $\overline{\mathfrak{N}}$ respectively. Since $\mathfrak{M}$ is R-projetive, there exists an R-homomorphism f of $\mathfrak{M}$ into $\mathfrak{N}$ such that $\nu f = \varphi_0 \mu$. Noting that ν maps $f(\mathfrak{M})$ onto $\overline{\mathfrak{N}}$ and $\mathfrak{N}N$ is the kernel of ν, we have $\mathfrak{N} = f(\mathfrak{M}) + \mathfrak{N}N$. Then by the above lemma we obtain $\mathfrak{N} = f(\mathfrak{M})$, that is, f maps $\mathfrak{M}$ onto $\mathfrak{N}$. This proves our assertion.

§ 3. Semi-linear normal basis

Let Δ be a division ring, and let Φ be a division subring of Δ. In the sequel, we suppose that Δ is Galois and finite over Φ, that is, Φ is the fixed subring of a group of antomorphisms of Δ, and $[\Delta : \Phi]_l$ $(= [\Delta : \Phi]_r) = n < +\infty$. By $\mathfrak{G}$ we denote the group of automorphisms of Δ wich leave Φ elementwise invariant. We shall say that $\mathfrak{G}$ is the Galois group of Δ over Φ.

Let $\mathfrak{E}$ be the ring of endomorphisms of Δ considered as an additive abelian group. Then $\mathfrak{E}$ ocntains $\mathfrak{G}$ and Δ_R (the ring of right multiplications of the elements of Δ), and it contains the ring $\mathfrak{G}\Delta_R$ generated by $\mathfrak{G}$ and Δ_R. Noting

that the formula

$$d_R \cdot \sigma = \sigma \cdot (d\sigma)_R \qquad d \in \Delta,\ \sigma \in \mathfrak{G}$$

holds, we shall see that every element a of $\mathfrak{G}\Delta_R$ is expressed as a finite sum

$$a = \sum_{\sigma \in \mathfrak{G}} \sigma d_{\sigma R}, \qquad d_\sigma \in \Delta.$$

Δ is naturally regarded as a right $\mathfrak{G}\Delta_R$-module.

Lemma 2. *$\mathfrak{G}\Delta_R$ is a simple ring with minimum condition having the capacity n and $\Delta^{(n)}$, the direct sum of n-fold copies of the right $\mathfrak{G}\Delta_R$-module Δ, is $\mathfrak{G}\Delta_R$-isomorphic to $\mathfrak{G}\Delta_R$.*

Proof. Since $\mathfrak{G}\Delta_R$ contains Δ_R, Δ is an irreducible right $\mathfrak{G}\Delta_R$-module, and as is easily seen the commutor ring of $\mathfrak{G}\Delta_R$ in $\mathfrak{E}$ is the left mutiplication ring Φ_L. Then by the density theorem for irreducible modules $\mathfrak{G}\Delta_R$ is a dense ring of linear transformations of the left Φ-vector space Δ. Since Δ has finite degree over Φ, this implies that $\mathfrak{G}\Delta_R$ is the ring of linear transformations of Δ over Φ. Thus $\mathfrak{G}\Delta_R$ is a simple ring with minimum condition having the capacity n. Noting that irreducible modules for a simple ring with minimum condition are all isomorphic, we obtain the latter half of the lemma.

As is clear from the above proof, we can apply the lemma to every automorphism group $\mathfrak{H}$ of Δ with Φ as its fixed subring.

When there exists an automorphism group $\mathfrak{G}_0 = \{\sigma_1 = 1, \cdots, \sigma_n\}$ of order n whose fixed subring is Φ, we shall say that Δ is strictly Galois over or more explicitly Δ is $\mathfrak{G}_0$-strictly Galois over Φ. Needless to say $\mathfrak{G}_0$ is a subgroup of $\mathfrak{G}$. The question whether every finite Galois extension is necessarily strictly Galois or not is still open.

Corollary 3. *Let Δ is $\mathfrak{G}_0$-strictly Galois over Φ. Then the right $\mathfrak{G}_0\Delta_R$-module $\Delta^{(n)}$ is $\mathfrak{G}_0\Delta_R$-isomorphic to $\mathfrak{G}_0\Delta_R$, and $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is a right basis of $\mathfrak{G}_0\Delta_R$ over Δ_R.*

Proof. Since $\mathfrak{G}_0\Delta_R = \mathfrak{G}\Delta_R$, the first part of the assertions is obvious. Let $\{l_1, \cdots, l_n\}$ be a left basis of Δ over Φ, and let d_i's be the linear transformations of the left Φ-vector space Δ defined by

$$(l_i)d_j = \delta_{ij} \qquad \text{(the Kronecker's delta)}.$$

Then, as is easily verified, $\mathrm{Hom}_\Phi(\Delta, \Delta)$, the ring of linear transformations of the Φ-space Δ, is $\sum_{i=1}^{n} \oplus d_i\Delta_R$ where d_i's are linearly independent over Δ_R. Since $\mathfrak{G}_0\Delta_R = \sum_{i=1}^{n} \sigma_i\Delta_R = \mathrm{Hom}_\Phi(\Delta, \Delta)$, $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is a right basis of $\mathfrak{G}_0\Delta_R$ over Δ_R as

asserted.

Now we are in the position to state our main theorem.

Theorem 3. *Let Δ be $\mathfrak{G}_0$-strictly Galois over Φ, and let $[\Delta:\Phi]_l=n<+\infty$. Suppose that Λ is a division subring of Δ which is invariant as a whole under $\mathfrak{G}_0$.*

(i) *If $[\Delta:\Lambda]_r=m<+\infty$, and $m=nq+r$ $(0\leqq r<n)$, then there exist $q+1$ elements $\xi_1,\cdots,\xi_q;\ \rho$ of Δ such that $\{\xi_i^\sigma;\ \sigma\in\mathfrak{G}_0,\ i=1,\cdots,q\}$ and suitable r elements in $\{\rho^\sigma;\ \sigma\in\mathfrak{G}_0\}$ form a right basis of Δ over Λ.*[3)]

(ii) *if $[\Delta:\Lambda]_r=\omega$, where ω is an infinite cardinal number, then there exist elements $\xi_\alpha(\alpha\in A)$ in Δ such that $\{\xi_\alpha^\sigma;\ \sigma\in\mathfrak{G}_0,\ \alpha\in A\}$ is a right basis of Δ over Λ, where A is an index set with the cardinal ω.*

Proof. Since Λ is invariant as a whole under $\mathfrak{G}_0$, every element a of $\mathfrak{G}_0\Lambda_R$ is expressed as a finite sum

$$a=\sum_{\sigma\in\mathfrak{G}_0}\sigma\lambda_{\sigma R},\qquad \lambda_\sigma\in\Lambda.$$

Let $\{u_1,\cdots,u_m\}$ be a right basis of Δ over Λ. Then we have

$$\mathfrak{G}_0\Delta_R=\Delta_R\mathfrak{G}_0=\sum_{i=1}^{m}u_{i_R}\Lambda_R\mathfrak{G}_0=\sum_{i=1}^{m}u_{i_R}\mathfrak{G}_0\Lambda_R$$

and, as is easily verified, $\{u_{1_R},\cdots,u_{m_R}\}$ is a right basis of the right $\mathfrak{G}_0\Lambda_R$-module $\mathfrak{G}_0\Delta_R$. Then by Corollary 1, we have a $\mathfrak{G}_0\Lambda_R$-isomorphism:

$$\Delta^{(n)}\cong(\mathfrak{G}_0\Lambda_R)^{(m)}.$$

Since $\mathfrak{G}_0\Lambda_R$ is a ring with minimum condition the results of Corollary 1 are applicable. Thus we have a $\mathfrak{G}_0\Lambda_R$-isomorphism:

$$\Delta\cong(\mathfrak{G}_0\Lambda_R)^{(q)}\oplus\mathfrak{m}$$

where $\mathfrak{m}$ is a $\mathfrak{G}_0\Lambda_R$-homomorphic image of $\mathfrak{G}_0\Lambda_R$.

Setting here ξ_i the element of Δ which corresponds to $(0,\cdots,0,\overset{i}{\check{1}},\cdots,0)$ and ρ the one which corresponds to the element m, the image of 1 under the $\mathfrak{G}_0\Lambda_R$-homomorphism of $\mathfrak{G}_0\Lambda_R$ onto $\mathfrak{m}$, then we see that the elements ξ_i's and ρ are the desired elements in (i).

If $[\Delta:\Lambda]_r=\omega$, then in the same way as in (i) we have a $\mathfrak{G}_0\Lambda_R$-isomorphism:

$$\Delta^{(n)}\cong(\mathfrak{G}_0\Lambda_R)^{(\omega)}.$$

Then, by Corollary 2 we obtain a $\mathfrak{G}_0\Lambda_R$-isomorphism:

3) Cf. [10].

$$\Delta \cong (\mathfrak{G}_0 \Delta_R)^{(\omega)}$$

and this implies the validity of our assertion (ii).

As a special case of Theorem 3 (i), we have

Corollary 4. *Let Δ, Φ and $\mathfrak{G}_0$ be as in Theorem 3. Then there exists an element ξ such that $\{\xi^\sigma; \sigma \in \mathfrak{G}_0\}$ is a right basis of Δ over Φ.*

Let Z be the center of Δ, and let T be the commutor ring of Φ in Δ. By $\mathfrak{I}$ we denote the subgroup of $\mathfrak{G}$ which consists of all inner automorphisms in $\mathfrak{G}$. It is well known that $(\mathfrak{G}:\mathfrak{I})\ [T:Z]=[\Delta:\Phi]=n$, and if $\{\sigma_1, \cdots, \sigma_r\}$ is a complete representative system of $\mathfrak{G}$ modulo $\mathfrak{I}$ and $\{\tau_1, \cdots, \tau_s\}$ is a basis of T over Z, then $\{\sigma_i I_{\tau_j} : i=1, \cdots, r; j=1, \cdots, s\}$ is a basis of $\mathfrak{G}\Delta_R$ over Δ_R where I_τ denotes the inner automorphism induced by the element τ.

In [5], Kasch obtained the following normal basis theorem in Noether's sense [5, Satz 9]:

Δ is $\mathfrak{G}\Delta_R$-isomorphic to $\mathfrak{G}\Delta_R$ if and only if $Z=T$ or $T \subseteqq \Phi$.

We shall try to generalize the theorem to the case of semi-linear normal basis theorem.

Lemma 3. *Let Λ be a division subring of Δ which is invariant as a whole under the Galois group $\mathfrak{G}$. If $[\Delta:\Lambda]_r$ is finite, then the following conditions (a), (b), (c) are equivalent.*

(a) $Z=T$ *or* $T \subseteqq \Lambda$

(b) $[\mathfrak{G}\Lambda_R : \Lambda_R]_r = [\Delta:\Phi]$

(c) $[\mathfrak{G}\Delta_R : \mathfrak{G}\Lambda_R]_r = [\Delta:\Lambda]_r$

Moreover (a) (or equivalently (b)) implies (c) without the finiteness condition of $[\Delta:\Lambda]_r$.

Proof. The proof of the equivalence of (a) and (b) proceeds quite analogously to that of [5, Satz 10] hence we shall omit it here. The equivalence holds in fact without the supposition $[\Delta:\Lambda]_r < +\infty$. The equivalence of (b) and (c) is clear from the relation

$$[\mathfrak{G}\Delta_R : \mathfrak{G}\Lambda_R]_r [\mathfrak{G}\Delta_R : \Lambda_R]_r = [\mathfrak{G}\Delta_R : \Delta_R]_r [\Delta_R : \Lambda_R]_r = [\Delta:\Phi][\Delta:\Lambda]_r .$$

The last part of the lemma is almost obvious.

Combining this lemma with Corollary 1, we obtain the following generalization of [5, Satz 9].

Theorem 4. *Let Δ be Galois and finite over Φ with the Galois group $\mathfrak{G}$, and let $[\Delta:\Phi]=n$. Suppose that Λ is a division subring of Δ which is invariant as a whole under $\mathfrak{G}$.*

(i) *If $[\Delta:\Lambda]_r = m < +\infty$, and $m=nq+r$ $(0 \leqq r < n)$, then the following*

propositions are equivalent:

(1) *There exists a* $\mathfrak{G}\Lambda_R$*-isomorphism*:

$$\Delta \cong (\mathfrak{G}\Lambda_R)^{(q)} \oplus \mathfrak{m}$$

where $\mathfrak{m}$ *is a* $\mathfrak{G}\Lambda_R$*-hmomorphic image of* $\mathfrak{G}\Lambda_R$ *such that* $\mathfrak{m}^{(n)} \cong (\mathfrak{G}\Lambda_R)^{(r)}$.

(2) $Z=T$ *or* $T \subseteqq \Lambda$.

(ii) *If* $[\Delta : \Lambda]_r = \omega$ (*infinite*) *and the condition* (2) *is satisfied, then there exists a* $\mathfrak{G}\Lambda_R$*-isomorphism*

$$\Delta \cong (\mathfrak{G}\Lambda_R)^{(\omega)} .$$

Corollary 5. *Let* Δ, Φ *and* $\mathfrak{G}$ *be as in Theorem* 4. *If* $Z=T$ *or* $T \subseteqq \Phi$, *then for any system* $\{\sigma_1, \cdots, \sigma_r ; I_{\tau_1}, \cdots, I_{\tau_s}\}$ *chosen from* $\mathfrak{G}$ *such that* $\{\sigma_1, \cdots, \sigma_r\}$ *is a complete representative system of* $\mathfrak{G}$ *modulo* $\mathfrak{H}$ *and* $\{\tau_1, \cdots, \tau_s\}$ *is a basis of* T *over* Z, *there exists an element* ξ *in* Δ *such that* $\{\xi^{\sigma_i I_{\tau_j}} : i=1, \cdots, r; j=1, \cdots, s\}$ *is a right basis of* Δ *over* Φ.

Let Λ be a subring of Δ which is invariant as a whole under $\mathfrak{G}$ such that $[\Delta : \Lambda]_r = m \leqq n$, and let $\{u_1, \cdots, u_m\}$ be a right basis of Δ over Λ. Then we have $\mathfrak{G}\Delta_R = \Delta_R\mathfrak{G} = \sum_{i=1}^{m} u_{i_R}\Lambda_R\mathfrak{G} = \sum_{i=1}^{m} u_{i_R}\mathfrak{G}\Lambda_R$, accordingly $\mathfrak{G}\Delta_R$ is $\mathfrak{G}\Lambda_R$-homomorphic to $(\mathfrak{G}\Lambda_R)^{(m)}$. Since $\Delta^{(n)}$ is $\mathfrak{G}\Lambda_R$-isomorphic to $\mathfrak{G}\Delta_R$, this implies that $\Delta^{(n)}$ is $\mathfrak{G}\Lambda_R$-homomorphic to $(\mathfrak{G}\Lambda_R)^{(m)}$. Then by Theorem 2 we obtain the following

Theorem 5. *Let* Δ, Φ, $\mathfrak{G}$ *and* Λ *be as in Theorem* 4. *If* $[\Delta : \Lambda]_r = m \leqq n$, *then* Δ *is* $\mathfrak{G}\Lambda_R$-homomorphic to $\mathfrak{G}\Lambda_R$. *Especially* Δ *is* $\mathfrak{G}\Phi_R$*-homomorphic to* $\mathfrak{G}\Phi_R$.

A subgroup of the Galois group $\mathfrak{G}$ which contains a right basis of $\mathfrak{G}\Delta_R$ over Δ_R was called independent in [5]. An independent subgroup is nothing but one whose fixed subring coincides with Φ.

Corollary 6. *Let* $\mathfrak{G}'$ *be an independent subgroup of* $\mathfrak{G}$, *and let* Λ *be a division subring of* Δ *which is invariant as a whole under* $\mathfrak{G}'$. *If* $[\Delta : \Lambda]_r \leqq n$, *then* Δ *is* $\mathfrak{G}'\Lambda_R$*-homomorphic to* $\mathfrak{G}'\Lambda_R$.

§ 4. An application

Let Δ be a finite dimensional central division algebra over Φ of degree δ: $[\Delta : \Phi] = \delta^2$. Suppose that P is a maximal subfield of Δ which has a primitive element ξ. over Φ Let, as in § 3, $\mathfrak{E}$ be the endomorphism ring of the additive group Δ. Then the commutor ring of $\Delta_L\Delta_R$ in $\mathfrak{E}$ is the multiplication ring $\Phi_L = \Phi_R$. As is seen from the proof of Lemma 2 we have a $\Delta_L\Delta_R$-isomorphism:

$$\Delta^{(\delta^2)} \cong \Delta_L \Delta_R = \Delta_L \otimes_\Phi \Delta_R .$$

Since $[\Delta : P] = \delta$, it follows

$$\Delta_L \Delta_R \cong (P_L P_R)^{(\delta^2)}$$

whence

$$\Delta^{(\delta^2)} \cong (P_L P_R)^{(\delta^2)} \qquad \text{as right } P_L P_R\text{-modules.}$$

Hence, by Corollary 1 there exists a $P_L P_R$-isomorphism:

$$\Delta \cong P_L P_R = P_L \otimes_\Phi P_R .$$

Since $P = \sum_{j=1}^{\delta-1} \xi^j \Phi$, $P_L P_R = \sum_{i,j=1}^{\delta-1} \xi_L^i \xi_R^j \Phi$. Considering the element η of Δ which corresponds to $1 \in \sum_{i,j=1}^{\delta-1} \xi_L^i \xi_R^j \Phi$ in the above isomorphism, we obtain the following theorem:[4]

Theorem 6. (Albert and Brauer). *Let Δ be a finite dimensional central division algebra over Φ of degree δ. Suppose P is a maximal subfield of Δ which has a primitive element ξ. Then there exists an element η in Δ such that $\{\xi^i \eta \xi^j ;\ i,\ j = 0, 1, \cdots, \delta - 1\}$ is a basis for Δ over Φ.*

References

[1] E. ARTIN, C. NESBITT and R. THRALL: Rings with Minimum Condition, University of Michigan, 1944.

[2] G. AZUMAYA: Tanjun-kan no Daisūteki Riron (Algebraic Theory of Simple Rings), Kawade-shobo, Tokyo, 1951.

[3] S. EILENBERG: Algebras of cohomologically finite dimension, Comment, Math. Helv., vol. 28 (1954).

[4] N.JACOBSON: Structure of Rings, Amer. Math. Soc. Colloquium Publ., vol. 37 (1956).

[5] F. KASCH: Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., vol. 126 (1953).

[6] T. NAKAYAMA: Daisūkei to Bibun (Algebraic Systems and Derivations), Kawade-shobo, Tokyo, (1848).

[7] T. NAKAYAMA: Semi-linear normal basis for quasi-fields, Amer. J. of Math., vol. 71 (1949).

[8] H. NAGAO and T. NAKAYAMA: On the structure of (M_0)- and (M_u)-modules, Math. Zeit., 59 Bd. (1953/54).

4) This result is stated in [4, Chap. VIII. Theorem 2], but our present proof does not use the existence of a vector whose order is the minimum polynomial. (Cf. N. Jacobson, Lectures in Abstract Algebra II, Chap. III, §3).

[9] T. ONODERA and H. TOMINAGA: On strictly Galois extensions of degree p^e over a division ring of characteristic p, Math. J. of Okayama Univ., vol. 7 (1957).

[10] T. ONODERA and H. TOMINAGA: A note on strictly Galois extension of primary rings, J. Fac. Sci. Hokkaidô Univ., ser 1 (1961).

Department of Mathemats,
Hokkaidô University

(Received November 22, 1963)