Chin. Ann. of Math.
1 (2) 1980

A FINITE STRUCTURE THEOREM BETWEEN PRIMITIVE RINGS AND ITS APPLICATION TO GALOIS THEORY

XU YONGHUA (SHU YONG-HUA)
(*Fudan University*)

Introduction

Let $\mathfrak{M}=\Sigma Fu_i$ be a vector space over division ring F, and P a subring of F, in which P is Galois, i.e., there exists a group G of automorphisms of F such that $I(G)=P$. Let G_0 be the group of inner automorphisms belonging to G. We denote the inner automorphism $x\to rxr^{-1}$ by I_r, $r\in F$. In this case we shall consider the algebra of the group G, $E'=\sum\limits_{I_{r_j}\in G_0}\Phi r_j$, where Φ is the center of F. Let $P'=C_F(E')$ be the centralizer of E' in F and $L(F, \mathfrak{M})$ the complete ring of F-linear transformations of vector space $\mathfrak{M}$ over F, $T_\nu(F, \mathfrak{M})$ the set of all elements of $L(F, \mathfrak{M})$ with rank$<\aleph_\nu$. Then we have the following results:

(I) $[F:P']_L=n<\infty$ if and only if $T_\nu(P', \mathfrak{M})=\sum\limits_{j=1}^{n}\oplus r_{jL}T_\nu(F, \mathfrak{M})$, where $r_j\in E'$, r_{jL} denotes the scalar left multiplication of r_j.

(II) $[P':P]_L=t<\infty$ if and only if $T_\nu(P, \mathfrak{M})=\sum\limits_{j=1}^{t}\oplus S_jT_\nu(P', \mathfrak{M})$, where S_j denotes an F-semi-linear automorphism of $\mathfrak{M}=\sum Fu_i$, whose associated isomorphism is $\psi_j\in G$.

(III) if there exist $T_\nu(P, \mathfrak{M})$, $T_\nu(P', \mathfrak{M})$ and $T_\nu(F, \mathfrak{M})$ satisfying the relations in (I) and (II), then the relations will hold for any suitable $T_\mu(P, \mathfrak{M})$, $T_\mu(P', \mathfrak{M})$ and $T_\mu(F, \mathfrak{M})$, in particular for $L(P, \mathfrak{M})$, $L(P', \mathfrak{M})$ and $L(F, \mathfrak{M})$.

(IV) if $[F:P]_L<\infty$, then $C_F(C_F(E'))=E'$, $[F:P']_L=\dim. E'$ and $[P':P]_L=[G/G_0]$, where dim. E' denotes the dimension of E' over Φ, $[G/G_0]$ the index of G_0 in G. In particular, when G is a Galois group, then $C_F(P')=C_F(P)=E'$.

(V) if $\widetilde{G}$ is another group of automorphisms of F such that $I(\widetilde{G})=I(G)=P$, then $[G/G_0]=[\widetilde{G}/\widetilde{G}_0]$, dim. $E'=$dim. $\widetilde{E}'$, where $\widetilde{E}'$ is the algebra of the group $\widetilde{G}$.

As a special case, if the subring P is the center Φ of F, then we obtain immediately the following well known theorem from the above (I): $L(\Phi, \mathfrak{M})=L(F, \mathfrak{M})\otimes_\Phi F_L$ if and only if $[F:\Phi]_L<\infty$.

Manuscript received January 2, 1980.

From our above theorem we can obtain the finite Galois theory of division rings.

1

At first we introduce some terms and symbols. Write $L(F, \mathfrak{M})$ for the ring of all F-linear transformations of left vector space $\mathfrak{M}$ over division ring and denote the rank of element ω of $L(F, \mathfrak{M})$ by $\rho(\omega)$. In this case we set $T_\nu(F, \mathfrak{M})=\{\omega\in L(F, \mathfrak{M})\mid \rho(\omega)<\aleph_\nu\}$. Let $C_F(P)$ be the centralizer of P in F, and B a set of automorphisms of $(\mathfrak{M}, +)$, then the set of all automorphisms of $(\mathfrak{M}, +)$, which can be commutative with all elements of B, is called the centralizer of B. Now let G be a group of automorphisms of F and ψ an element of G, then it is easy to determine an F-semi-linear automorphism S of $\mathfrak{M}=\sum Fu_i$ by ψ, which is associated with S. In fact, let ω be any unit of $L(F, \mathfrak{M})$, then we denote S the correspondence $\sum\limits_{i<\infty} f_iu_i\to\sum\limits_{i<\infty} f_i^\psi(u_i\omega)$, it is clear that S is an F-semi-linear automorphism of $\mathfrak{M}$ with its associated isomorphism ψ. If we wish to indicate ψ explicitly, we denote $S=(S, \psi)$.

Now we consider the following set Θ

$$\Theta=\{S\mid S=(S, \psi), \ \psi\in G\} \tag{1}$$

and choose the S in the following way: if ψ is an inner automorphism belonging to G, i.e., $\psi=I_r=r_Lr_R^{-1}\in G$, then we set $S=r_L$, the left scalar multiplication of element r, if $\psi=1\in G$, then set $S=(S, 1)$, the identity of $L(F, \mathfrak{M})$. It is clear that Θ is a set of F-semi-linear automorphisms of $\mathfrak{M}$ with identity. Put $\Theta^{-1}=\{S^{-1}\mid S\in\Theta\}$, and denote $[\Theta]$ the multiplicative group generatedby Θ and Θ^{-1}.

Definition 1 *Let $\mathfrak{M}=\sum Fu_i$, G be a group of automorphisms of division ring F, G_0 be the group of inner automorphisms belonging to G. Then we call the multiplicative group $[\Theta]$ the group of F-semi-linear automorphisms associated with G and as usual call $E'=\sum\limits_{I_{r_j}\in G_0}\Phi r_j$ the algebra of G, where Φ is the center of F.*

From now on "module" and "vector space" will always mean a right module and a left infinite vector space respectively.

Now we explain what is the meaning of the rank of a matrix $(a_{ij})_{n\times m}$ over a division ring F. We say that a matrix $(a_{ij})_{n\times m}$ over a division ring F has full rank if and only if $(a_{ij})_{n\times m}$ can be transformed into such $(a'_{ij})_{n\times m}$ by usual elementary operations, where $a'_{ii}=1$, $a'_{ij}=0$, $i>j$, $j=1, \cdots, m$; $i=1, \cdots, n$, $n\leqslant m$.

Then we can formulate the following lemma:

Lemma 1 *Let $\mathfrak{M}=\sum Fu_i$ be a vector space over division ring F, $y_1, \cdots, y_n$ be n F-linearly independent elements of $\mathfrak{M}$. Suppose that the following system of linear equations*

$$\sum_{j=1}^{m} a_{ij}x_j=y_i, \ i=1, \cdots, n, \ a_{ij}\in F$$

has solution in $\mathfrak{M}$, *then* $m \geqslant n$ *and* $(a_{ij})_{n\times m}$ *has full rank, we may assume for example* $(a_{ij})_{n\times n}$ *has full rank,* $i, j=1, \cdots, n$. *Then the system of linear equations* $\sum_{j=1}^{n} a_{ij}X_j = Y_i$, $i=1, \cdots, n$ *has solution in* $\mathfrak{M}$ *for any* n *elements* $Y_1, \cdots, Y_n$ *of* $\mathfrak{M}$ *and its solution can be expressed as* $X_i = \sum_{j=1}^{n} b_{ij}Y_j$, $i=1, \cdots, n$, $b_{ij}\in F$.

proof See [1].

Now we can prove the following main theorem:

Theorem 1 *Let* $\mathfrak{M} = \sum Fu_i$ *be a vector space over a division ring* F, G *a group of automorphisms of* F, G_0 *the inner automorphisms belonging to* G. *Let* E' *be the algebra of* G, $[\Theta]$ *the group of* F*-semi-linear automorphisms associated with* G. *Let* $P' = C_F(E')$, $P = I(G) = \{f\in F \mid f^{\psi}=f, \text{ for all } \psi \in G\}$. *Denote* $L(F, \mathfrak{M})$, $L(P', \mathfrak{M})$ *and* $L(P, \mathfrak{M})$ *the ring of all* F-, P'- *and* P*-linear transformations of* $\mathfrak{M}$ *respectively,* $T_\nu(F, \mathfrak{M})$, $T_\nu(P', \mathfrak{M})$ *and* $T_\nu(P, \mathfrak{M})$ *the rings of all elements with ranks* $< \aleph_\nu$. *Then we have the following results:*

(I) $[F:P']_L = n < \infty$ *if and only if*

$$T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} \oplus r_{jL} T_\nu(F, \mathfrak{M}), \ r_j \in E'. \tag{2}$$

Moreover, if $[F:P']_L = n<\infty$ *and* $T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} r'_{jL}T_\nu(F, \mathfrak{M})$ *for* n *elements* $r'_1, \cdots, r'_n$ of E', *then*

$$\sum_{j=1}^{n} r'_{jL}T_\nu(F, \mathfrak{M}) = \sum_{j=1}^{n} \oplus r'_{jL}T_\nu(F, \mathfrak{M})$$

(II) $[P':P]_L = t < \infty$ *if and only if*

$$T_\nu(P, \mathfrak{M}) = \sum_{k=1}^{t} \oplus S_k T_\nu(P', \mathfrak{M}), \ S_k \in [\Theta] \tag{3}$$

Moreover, if $[P':P]_L = t<\infty$ *and* $T_\nu(P, \mathfrak{M}) = \sum_{k=1}^{t} S'_j T_\nu(P', \mathfrak{M})$ *for elements* $S'_1, \cdots, S'_t$ *of* $[\Theta]$, *then* $\sum_{k=1}^{t} S'_k T_\nu(P', \mathfrak{M}) = \sum_{k=1}^{t} \oplus S'_k T_\nu(P', \mathfrak{M})$.

(III) *if the relations* (2) *and* (3) *are true, then*

$$T_\nu(P, \mathfrak{M}) = \sum_{k=1,\cdots,t;\, j=1,\cdots,n} \oplus S_k r_{jL} T_\nu(F, \mathfrak{M}). \tag{4}$$

(IV) *if there exists an ordinal number* ν *such that* $T_\nu(P, \mathfrak{M})$, $T_\nu(P', \mathfrak{M})$ *and* $T_\nu(F, \mathfrak{M})$ *satisfy the relations in* (I) *and* (II), *then the relations still hold for any* $T_\mu(P, \mathfrak{M})$, $T_\mu(P', \mathfrak{M})$ *and* $T_\mu(F, \mathfrak{M})$, *in particular, for* $L(P, \mathfrak{M})$, $L(P', \mathfrak{M})$ *and* $L(F, \mathfrak{M})$.

Proof First we prove (I). It is clear that $E'_L T_\nu(F, \mathfrak{M}) = \{\sum_{j<\infty} e'_{jL}\omega \mid e'_{jL}\in E'_L, \omega_j \in T_\nu(F, \mathfrak{M})\}$ is a ring, where $E'_L = \{e'_L \mid e' \in E'\}$, and $\mathfrak{M}$ evidently an irreducible $E'_L T_\nu(F, \mathfrak{M})$-module. It is easy to see that $P' = C_F(F')$ is the centralizer of $E'_L T_\nu(F, \mathfrak{M})$. Let $[F:P']_L = n < \infty$, then $F = \sum_{\alpha=1}^{n} P' f^{(\alpha)}$, $f^{(\alpha)} \in F$. Now we want to prove that

$$T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} \oplus r_{jL} T_\nu(F, \mathfrak{M}),\ r_j \in F'.$$

In fact, $$\mathfrak{M} = \sum_i F u_i = \sum_{\alpha, i} P' v_i^{(\alpha)},\ v_i^{(\alpha)} = f^{(\alpha)} u_i,\ i \in \Gamma.$$

Let $y_1, \cdots, y_n$ be any F-linearly independent elements. Since $E'_L T_\nu(F, \mathfrak{M})$ is a dense subring of $L(P', \mathfrak{M})$ and $v_i^{(1)}, \cdots, v_i^{(n)}$ are P'-linearly independent elements, there exists an element $\sigma \in E'_L T_\nu(F, \mathfrak{M})$ such that $v_i^{(\alpha)} \sigma = y_\alpha$, $\alpha = 1, \cdots, n$. Since $\sigma = \sum_{j=1}^{m} r_{jL} \sigma'_j$, $r_j \in E'$, $\sigma'_j \in T_\nu(F, \mathfrak{M})$, we have

$$y_\alpha = v_i^{(\alpha)} \sigma = \sum_{j=1}^{m} r_j f^{(\alpha)} (u_i \sigma'_j),\ \alpha = 1, \cdots, n. \tag{5}$$

Put $a_{\alpha j} = r_j f^{(\alpha)}$, $x_j = u_i \sigma'_j$, then (5) has the form

$$\sum_{j=1}^{m} a_{\alpha j} x_j = y_\alpha,\ \alpha = 1, \cdots, n. \tag{6}$$

Since the equation (6) has solution and $y_1, \cdots, y_n$ are F-linearly independent, it follows by lemma 1 that $(a_{ij})_{n \times m}$ has full rank. Without loss of generality we may assume that $(a_{ij})_{n \times n}$ has full rank, $i, j = 1, \cdots, n$.

Now we want to show that every element σ^* in $T_\nu(P', \mathfrak{M})$ can be written as $\sigma^* = \sum_{j=1}^{n} r_{jL} \sigma''_j$, where r_{jL} are the same elements as in the above form $\sigma = \sum_{j=1}^{m} r_{jL} \sigma'_j$ and $\sigma''_j \in T_\nu(F, \mathfrak{M})$.

Put $v_i^{(\alpha)} \sigma^* = Y_\alpha(i)$, $\alpha = 1, \cdots, n$, and consider the following system of equations

$$\begin{gathered} \sum_{j=1}^{n} a_{\alpha j} X_j(i) = Y_\alpha(i),\ a_{\alpha j} = r_j f^{(\alpha)}, \\ \alpha = 1, \cdots, n,\ i \in \Gamma. \end{gathered} \tag{7}$$

Then by lemma 1 there exist solutions $X_1(i), \cdots, X_n(i)$ of (7) for any $i \in \Gamma$. Since $\{u_i\}_\Gamma$ is an F-base of $\mathfrak{M}$ and $\rho(\sigma^*) < \aleph_\nu$, there exists an element $\sigma'_j \in T_\nu(F, \mathfrak{M})$ for any fixed j such that

$$u_i \sigma'_j = X_j(i),\ i \in \Gamma.$$

Put $\bar{\sigma} = \sum_{j=1}^{n} r_{jL} \sigma'_j$, then it follows that $v_i^{(\alpha)} \bar{\sigma} = \sum_{j=1}^{n} a_{\alpha j} X_j(i) = v_i^{(\alpha)} \sigma^*$. This shows that $\sigma^* = \bar{\sigma} \in \sum_{j=1}^{n} r_{jL} T_\nu(F, \mathfrak{M})$. It is easy to see that $T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} r_{jL} T_\nu(F, \mathfrak{M})$, $r_j \in E'$.

Further, if $\sum_{j=1}^{n} r_{jL} \omega_j = 0$, $\omega_j \in T_\nu(F, \mathfrak{M})$, then we have

$$0 = (f^{(\alpha)} u_i) \sum_{j=1}^{n} r_{jL} \omega_j = \sum_{j=1}^{n} a_{\alpha j} X_j(i),\ X_j(i) = u_i \omega_j.$$

Since $(a_{\alpha j})_{n \times n}$ has full rank, we have $X_j(i) = u_i \omega_j = 0$, $i \in P$, it follows that $\omega_j = 0$, $j = 1, \cdots, n$. This shows that $T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} \oplus r_{jL} T_\nu(F, \mathfrak{M})$.

On the contrary, if $T_\nu(P', \mathfrak{M}) = \sum_{j=1}^{n} \oplus r_{jL} T_\nu(F, \mathfrak{M})$, $r_j \in E'$, then we shall show $[F : P'] \leqslant n$. In fact, if we put $F = \sum_{\alpha \in I} P' f^{(\alpha)}$, where $\{f^{(\alpha)}\}_I$ is a base of F, then we have

$\mathfrak{M}=\sum_{\substack{i\in\Gamma\\ \alpha\in I}} P'v_i^{(\alpha)}$, $v_i^{(\alpha)}=f^{(\alpha)}u_i$. If $[F:P']>n$ were true and $v_i^{(1)}, \cdots, v_i^{(u)}, v_i^{(u+1)}$ were P'-linearly independent, then for any $n+1$ F-linearly independent elements $y_1, \cdots, y_{n+1}$ of $\mathfrak{M}$ we could find an element $\sigma\in T_\nu(P', \mathfrak{M})$ such that $y_\alpha=v_i^{(\alpha)}\sigma$, $\alpha=1, \cdots, n+1$, by assumption $\sigma=\sum_{i=1}^{n} r_{jL}\omega_j$, $\omega_j\in T_\nu(F, \mathfrak{M})$, hence we have

$$y_\alpha=\sum_{j=1}^{n} r_j f^{(\alpha)}(u_i\omega_j)=\sum_{j=1}^{n} a_{\alpha j}x_j, \qquad (8)$$
$$\alpha=1, \cdots, n+1,$$

where $a_{\alpha j}=r_j f^{(\alpha)}$, $x_j=u_i\omega_j$. Since the system of equations of (8) has solution x_j and $y_1, \cdots, y_{n+1}$ are F-linearly independent, we have a contradiction with $n\geqslant n+1$. This shows that $[F:P']_L=n'\leqslant n$.

We shall now show $n'=n$. In fact, put $F=\sum_{\alpha=1}^{n'} P'f^{(\alpha)}$, $\mathfrak{M}=\sum Fu_i=\sum_{\substack{\alpha=1,\cdots,n'\\ i\in\Gamma}} P'v_i^{(\alpha)}$, $v_i^{(\alpha)}=f^{(\alpha)}u_i$, it is clear that there exist elements $E_i\in L(F, \mathfrak{M})$ such that $u_jE_i=\delta_{ij}\, u_i$ and elements $e_{i\alpha}\in L(P', \mathfrak{M})$ such that

$$v_{i'}^{(\alpha')}e_{i\alpha}=v_i^{(\alpha)}, \text{if } i=i', \ \alpha=\alpha',$$
$$v_{i'}^{(\alpha')}e_{i\alpha}=0, \text{ if } i\neq i', \text{ or } \alpha\neq\alpha'.$$

It is easy to see that $E_iL(F, \mathfrak{M})$ and $e_{i\alpha}L(P', \mathfrak{M})$ are minimal right ideals of $T_\nu(F, \mathfrak{M})$ and $T_\nu(P', \mathfrak{M})$ respectively. Thus we have

$$E_iT_\nu(P', \mathfrak{M})=\sum_{\alpha=1}^{n'} e_{i\alpha}T_\nu(P', \mathfrak{M}). \qquad (9)$$

Now we shall prove that $e_{i\alpha}T_\nu(P', \mathfrak{M})=e_{i\alpha}T_\nu(F, \mathfrak{M})$. In fact, we denote by σ' any element of $T_\nu(P', \mathfrak{M})$, then it is clear that for any fixed pair i and α we can always find an element $\omega\in T_\nu(F, \mathfrak{M})$ such that $v_i^{(\alpha)}e_{i\alpha}\omega=v_i^{(\alpha)}e_{i\alpha}\sigma'$. Thus we have $v_j^{(\beta)}e_{i\alpha}\omega=v_j^{(\beta)}e_{i\alpha}\sigma'$ for any $j\in\Gamma$, $\beta=1, \cdots, n'$. It follows therefore that $e_{i\alpha}\sigma'=e_{i\alpha}\omega$, $e_{i\alpha}T_\nu(P', \mathfrak{M})=e_{i\alpha}T_\nu(F, \mathfrak{M})$.

Next we shall show that $e_{i\alpha}T_\nu(F, \mathfrak{M})$ is an irreducible $T_\nu(F, \mathfrak{M})$-module. If $e_{i\alpha}\omega T_\nu(F, \mathfrak{M})\neq 0$, $\omega\in T_\nu(F, \mathfrak{M})$, then it follows from the property of the minimal right ideal $E_iT_\nu(F, \mathfrak{M})$ in $T_\nu(F, \mathfrak{M})$ that $e_{i\alpha}\omega T_\nu(F, \mathfrak{M})=e_{i\alpha}E_i\omega T_\nu(F, \mathfrak{M})=e_{i\alpha}T_\nu(F, \mathfrak{M})$.

It follows from (9) that

$$E_iT_\nu(P', \mathfrak{M})=\sum_{\alpha=1}^{n'} \oplus e_{i\alpha}T_\nu(F, \mathfrak{M}). \qquad (10)$$

This shows that $T_\nu(P', \mathfrak{M})$ has height 1 and index $n'=[F:P']_L$ over $T_\nu(F, \mathfrak{M})$.

On the other hand, we know that $T_\nu(P', \mathfrak{M})=\sum_{j=1}^{n}\oplus r_{jL}T_\nu(F, \mathfrak{M})$, $r_j\in E'$. Since

$$E_ir_{jL}T_\nu(F, \mathfrak{M})\cap\Big(\sum_{k\neq j} E_ir_{kL}T_\nu(F, \mathfrak{M})\Big)=0,$$

we have

$$E_iT_\nu(P', \mathfrak{M})=\sum_{j=1}^{n}\oplus E_ir_{jL}T_\nu(F, \mathfrak{M}). \qquad (11)$$

This shows that the index n' of $T(P', \mathfrak{M})$ over $T(F, \mathfrak{M})$ is not smaller than n.

To show the final assertion of (I), we put $[F:P']_L=n$, $\mathfrak{M}=\sum_{\Gamma} Fu_i=\sum_{\substack{\alpha=1\\ i\in\Gamma}}^{n} P'v_i^{(\alpha)}$, $v_i^{(\alpha)}=f^{(\alpha)}u_i$, then for arbitrary n F-linearly independent elements $y_1, \cdots, y_n$ of $\mathfrak{M}$, there exists an element $\sigma\in T_\nu(P', \mathfrak{M})$ such that $y_\alpha=v_i^{(\alpha)}\sigma$. But $T_\nu(P', \mathfrak{M})=\sum_{j=1}^{n} r_{jL}T_\nu(F, \mathfrak{M})$ is given, hence $\sigma=\sum_{j=1}^{n} r_{jL}\omega_j$, $\omega_j\in T_\nu(F, \mathfrak{M})$. It follows $y_\alpha=\sum_{j=1}^{n} a_{\alpha j}x_j$, $a_{\alpha j}=r_jf^{(\alpha)}$, $u_i\omega_j=x_j$, $\alpha=1, \cdots, n$. By lemma 1, $(a_{ij})_{n\times n}$ has full rank. As in the proof of the preceding assertion we can show, if $\sum_{j=1}^{n} r_{jL}\omega'_j=0$, $\omega'_j\in T_\nu(F, \mathfrak{M})$, then it must be $\omega'_j=0$, this shows $\sum_{j=1}^{n} r_{jL}T_\nu(F, \mathfrak{M})=\sum_{j=1}^{n}\oplus r_{jL}T_\nu(F, \mathfrak{M})$.

Thus the proof of part (I) of theorem is now complete.

(II) First we suppose that $[P':P]_L=t<\infty$. It follows $P'=\sum_{\alpha=1}^{t} Pf_\alpha$, hence $\mathfrak{M}=\sum_{j\in\Gamma'} P'w_j=\sum_{\substack{\alpha=1\\ i\in\Gamma'}}^{t} Pv_i^{(\alpha)}$, $v_i^{(\alpha)}=f'_\alpha w_i$. It is clear that $\{v_i^{(\alpha)}\}$ is a P-base of $\mathfrak{M}$. By assumption of the theorem $E'=\sum_{I_{r_j}\in G_0}\Phi r_j$ is the algebra of G. It is easy to prove $E'^{\psi}=E'$, where $\psi\in G$. In fact, if $I_r\in G_0$, then $I_{r^\psi}\psi^{-1}=\psi^{-1}I_r\in G$, hence $I_{r^\psi}\in G_0$, this follows that $r^\psi\in E'$, $E'^\psi\subset E'$. In the same way we can obtain $E'^{\psi^{-1}}\subseteq E'$. It follows therefore that $E'^\psi=E'$. On the other hand, by the definition $P'=C_F(E')$ we see that for every $\psi\in G$, there exists $P'^\psi=P'$. Now we consider the group $[\Theta]$ of F-semilinear automorphisms associated with G. Let $S\in[\Theta]$ and $S=(S, \psi)$. According to the preceding formulation we see that S is a P'-semi-linear automorphism of $\mathfrak{M}$. Now we make a correspondence $\sigma':\omega'\to S\omega'S^{-1}$ for ω' in $L(P', \mathfrak{M})$, it is easy to show that σ' is a ring automorphism of $L(P', \mathfrak{M})$. Hence $S\omega'=\omega'^{\sigma'}S$, $SL(P', \mathfrak{M})=L(P', \mathfrak{M})S$. Choose any element S_1 of $[\Theta]$ and assume that the associated isomorphism ψ with S and the ψ_1 with S_1 are identical in P', then there exists a unit l of $L(P', \mathfrak{M})$ such that $Sl=S_1$. In fact, let $\{w_j\}$ be a base of $\mathfrak{M}$ over P', it is clear that $\{w_jS\}$ and $\{w_jS_1\}$ are also P'-bases of $\mathfrak{M}$, hence there exists an element l in $L(P, \mathfrak{M})$ such that $w_jSl=w_jS_1$. It follows from the identity of ψ with ψ_1 in P' that $(\sum_{i<\infty} f'_iw_i)Sl=(\sum_{i<\infty} f'_iw_i)S_1$ for any $f'\in P'$. Thus $Sl=S_1$, $SL(P', \mathfrak{M})=S_1L(P', \mathfrak{M})$. According to the above statement we see

$[\Theta]L(P', \mathfrak{M})=\{\sum_{j<\infty} S_j\omega'_j \mid S_j\in[\Theta],\ \omega'_j\in L(P', \mathfrak{M})\}$ is a ring, and by its structure we know that $[\Theta]L(P', \mathfrak{M})=\sum_{S_j\in\Theta} S_jL(P', \mathfrak{M})$. Thus $[\Theta]T_\nu(P', \mathfrak{M})=\sum_{S_j\in\Theta} S_jT_\nu(P', \mathfrak{M})$.

On the other hand, we see that $P_L=I(G)_L$ is the centralizer of $[\Theta]T_\nu(P', \mathfrak{M})$. Hence the ring $\sum_{S_j\in\Theta} S_jT_\nu(P', \mathfrak{M})$ is a dense subring of $L(P, \mathfrak{M})$. Let $y_1, \cdots, y_t$ be t P'-linearly independent elements of $\mathfrak{M}=\sum_{\alpha=1}^{t} Pv_i^{(\alpha)}=\sum_{\Gamma'} P'w_j$, then there exists an element $\sigma\in\sum_{S_j\in\Theta} S_jT_\nu(P', \mathfrak{M})$ such that $v_i^{(\alpha)}\sigma=y_\alpha$, $\alpha=1, \cdots, t$. But $\sigma=\sum_{j=1}^m S'_j\sigma'_j$, $\sigma'_j\in T_\nu$ $(P', \mathfrak{M})$, we have therefore

$$y_\alpha=v_i^{(\alpha)}\sigma=\sum_{j=1}^m f_\alpha'^{\psi_j}(w_jS_j\sigma'_j)=\sum_{j=1}^m a_{\alpha j}x_j(i),\ i\in P', \tag{12}$$

where $a_{\alpha j}=f_\alpha'^{\psi_j}$, $f'_\alpha\in P'$, $x_j(i)=w_i(S_j\sigma'_j)$, $\alpha=1, \cdots, t$. Since the system of equations (12) has solution and $y_1, \cdots, y_t$ are P'-linearly independent, by the lemma 1 we have $m\geqslant t$ and $(a_{\alpha j})_{t\times m}$ with full rank. Now we may assume that $(a_{\alpha j})_{t\times t}$ has full rank, α, $j=1, \cdots, t$. Let $\sigma^*\in T_\nu(P, \mathfrak{M})$, $Y_\alpha(i)=v_i^{(\alpha)}\sigma^*$, $\alpha=1, \cdots, t$, then we consider the following system of equations

$$\sum_{j=1}^t a_{\alpha j}X_j(i)=Y_\alpha(i),\ a_{\alpha j}=f_\alpha'^{\psi_j},\ \alpha=1, \cdots, t. \tag{13}$$

By lemma 1 we see that (13) has a solution $X_j(i)$. For $S_j\in\Theta$ we see that $\{w_iS_j\}_{\Gamma'}$ is a P'-base of $\mathfrak{M}$, hence for any j there exists an element $\sigma''_j\in L(P', \mathfrak{M})$ such that $w_iS_j\sigma''_j=X_j(i)$, $i\in\Gamma'$. Since $\rho(\sigma^*)<\aleph_\nu$, the rank of the vector space $\sum_{i\in\Gamma} P'X_j(i)$ is smaller than $\aleph_\nu$, therefore $\sigma''_j\in T_\nu(P', \mathfrak{M})$. Put $\bar\sigma=\sum_{j=1}^t S_j\sigma_j$, we have

$$v_i^{(\alpha)}\bar\sigma=\sum_{j=1}^t f_\alpha'^{\psi_j}(w_iS_j\sigma''_j)=\sum_{j=1}^t a_{\alpha j}X_j(i)=v_i^{(\alpha)}\sigma^*,\ i\in\Gamma'.$$

This shows that $\sigma^*=\bar\sigma\in\sum_{j=1}^t S_jT_\nu(P', \mathfrak{M})$. It follows $T_\nu(P, \mathfrak{M})=\sum_{j=1}^t S_jT_\nu(P', \mathfrak{M})$. Using the same method as in (I) we can prove that $T_\nu(P, \mathfrak{M})=\sum_{j=1}^t \oplus S_jT_\nu(P', \mathfrak{M})$.

Next we assume that $T_\nu(P, \mathfrak{M})=\sum_{j=1}^t \oplus S_jT_\nu(P', \mathfrak{M})$, $S_j\in[\Theta]$. By the same method as in (I) we can show that $[P':P]_L=t$.

The final assertion in part (II) can be proved by repeating the method in (I). Thus the proof of part (II) is now complete.

Now we are going to prove part (III).

(III) Since $F=\sum_{\alpha=1}^n P'f^{(\alpha)}$, $P'=\sum_{\beta=1}^t Pg'^{(\beta)}$, we have $\mathfrak{M}=\sum_\Gamma Fu_i=\sum_{\substack{i\in\Gamma\\ \alpha=1,\cdots,n;\beta=1,\cdots,t}} P(g'^{(\beta)}f^{(\alpha)}u_i)$. Put $v_i^{(\alpha,\beta)}=g'^{(\beta)}f^{(\alpha)}u_i$. It is clear that $v_i^{(1,1)}, \cdots, v_i^{(t,n)}$ are P-linearly independent elements. Denote $y_{i,1}, \cdots, y_{t,n}$ a system of F-linearly independent elements, then there exists an element $\sigma\in T_\nu(P, \mathfrak{M})$ such that

$$y_{\beta,\alpha}=v_i^{(\beta,\alpha)}\sigma,\ \beta=1, \cdots, t;\ \alpha=1, \cdots, n.$$

By (I) and (II) we see that $\sigma=\sum_{\substack{k=1,\cdots,t\\ j=1,\cdots,n}} S_kr_{jL}\omega_{kj}$, $\omega_{kj}\in T_\nu(F, \mathfrak{M})$, hence we have

$$y_{\beta,\alpha}=\sum_{k,j}(g'^{(\beta)}f^{(\alpha)}u_j)S_kr_{jL}\omega_{kj}=\sum g'^{(\beta)\psi_kI_{r_j}}f^{(\alpha)\psi_kI_{r_j}}(u_iS_kr_{jL}\omega_{kj}).$$

Put $a_{kj}^{(\beta,\alpha)}=g'^{(\beta)\psi_kI_{r_j}}f^{(\alpha)\psi_kI_{r_j}}$, $X_{kj}^{(i)}=u_iS_kr_{jL}\omega_{kj}$, then the above equations can be formulated as follows

$$y_{\alpha,\beta}=\sum_{k,j}a_{kj}^{(\beta,\alpha)}X_{kj}(i),\ \beta=1, \cdots, t;\ \alpha=1, \cdots, n,\ i\in\Gamma. \tag{14}$$

By repetition of our argument of part (I) we can prove that $(a_{kj}^{(\beta,\alpha)})_{tn\times tn}$ has full rank.

If $\sum_{k,j} S_k r_{jL}\omega_{kj}=0$, where $\omega_{kj}\in T_\nu(F, \mathfrak{M})$, then we have

$$\sum_{k,j} a_{kj}^{(\beta,\alpha)} X_{kj}(i)=0,\ i\in\Gamma. \tag{15}$$

From the property of full rank of $(a_{kj}^{(\beta,\alpha)})_{nt\times nt}$ it follows that $X_{kj}(i)=0=u_i S_k r_{jL}\omega_{kj}$, $i\in\Gamma$. Therefore, $S_k r_{jL}\omega_{kj}=0$, this shows that $\sum_{k,j} S_k r_{jL} T_\nu(F, \mathfrak{M})=\sum_{k,j}\oplus S_k r_{jL} T_\nu(F, \mathfrak{M})$.

Suppose that $\sum_{\substack{k=1,\cdots,t\\ j=1,\cdots,n}} S'_k r'_{jL} T_\nu(F, \mathfrak{M})=T_\nu(P, \mathfrak{M})$, where $S'_k\in[\Theta]$, $r'_j\in E'$, then we can similarly prove that $T_\nu(P, \mathfrak{M})=\sum_{\substack{k=1,\cdots,t\\ j=1,\cdots,n}}\oplus S'_k r'_{jL} T_\nu(F, \mathfrak{M})$. Thus the proof of part (III) is complete.

It remains to prove that the part (IV) is true. As to the proof of the assertion of (IV), it follows directly from the course of the proof of the assertion of part (I).

Thus the proof of the theorem is complete.

Our theorem includes the following well known results.

Corollary 1 *Let $\mathfrak{M}=\sum Fu_i$ be a vector space over a division ring F, Φ the center of F. Then $[F:\Phi]_L=n<\infty$ if and only if $L(\Phi, \mathfrak{M})=F_L\otimes_\Phi L(F, \mathfrak{M})=\sum_{j=1}^{n}\oplus r_{jL}L(F, \mathfrak{M})$, where F_L denote the left scalar multiplication of F, $r_{jL}\in F_L$.*

Proof Let G be the group of all inner automorphisms of F. Then we have $I(G)=\Phi$. According to the assumption we have $P'=P=\Phi$. Therefore our assertion follows at once from theorem 1.

From the proof of theorem 1 we can immediately obtain the following results.

Corollary 2 *Let $\mathfrak{M}=\sum Fu_i$ be a vector space over F, E a subring of F, $C_F(E)=P$. Suppose that $[F:P]_L=n<\infty$, then the right dimension of $T_\nu(P, \mathfrak{M})$ over $T_\nu(F, \mathfrak{M})$ is n and the (right) height of $T_\nu(P, \mathfrak{M})$ over $T_\nu(F, \mathfrak{M})$ is 1, the (right) index is n.*

Corollary 3 *Let F be a division ring, G be a group of automorphisms of F, E' the algebra of G, $C_F(E')=P'$, then any element ψ of G induces an automorphism of P' and E'.*

2

Lemma 2 *Let $\mathfrak{M}=\sum Fu_i$, G be a group of automorphisms of F, E' the algebra of G, $P'=C_F(E')$, $P=I(G)$. Then $L(P, \mathfrak{M})=\sum_{k=1}^{t}\oplus S_k L(P', \mathfrak{M})$. Suppose that S is any P'-semi-linear transformation of $\mathfrak{M}$ and S in $L(P, \mathfrak{M})$, then there exists an element S_k of $S_1, \cdots, S_t$ such that $S=S_k r_L\omega$, $\psi=\tilde{\psi}_k I_r$, where ψ and $\tilde{\psi}_k$ are the associated isomorphisms of P' with S and S_k respectively and $\omega\in L(P', \mathfrak{M})$, $r\in C_{P'}(P)$.*

Proof By assumption of our lemma and theorem 1 we see that $S=\sum_{k=1}^{t} S_k\omega_k$, $\omega_k\in L(P', \mathfrak{M})$. Put $f'\in P'$, $u\in\mathfrak{M}$ and $uS\neq 0$, then we have

$$(f'u)S=\sum_{k=1}^{t} f'^{\psi_k}(uS_k\omega_k)=\sum_{k=1}^{t} f'^{\psi}(uS_k\omega_k). \tag{16}$$

Put $v_k=uS_k\omega_k$ and suppose that $v_1, \cdots, v_{t'}$ are P'-linearly independent elements and $v_{t'+j}=\sum_{i=1}^{t'} g_i'^{(t'+j)}v_i$ where $g_i'^{(t'+j)}\in P'$, $j=1, \cdots, t-t'$. Now we put the $v_{t'+j}$ into (16), we have

$$\sum_{k=1}^{t} f'^{\psi_k}v_k=\sum_{k=1}^{t'}(f'^{\psi_k}+\sum_{j=1}^{t-t'} f'^{\psi_{t'+j}}g_k'^{(t'+j)})v_k=\sum_{k=1}^{t'} f'^{\psi}(1+\sum_{j=1}^{t-t'} g_k'^{(t'+j)})v_k.$$

Since $v_1, \cdots, v_{t'}$ are P'-linearly independent elements, it follows that

$$f'^{\psi_k}+\sum_{j=1}^{t-t'} f'^{\psi_{t'+j}}g_k'^{(t'+j)}=f'^{\psi}(1+\sum_{j=1}^{t-t'} g_k'^{(t'+j)}),\quad k=1, \cdots, t'.$$

Suppose that $1+\sum_{j=1}^{t-t'} g_k'^{(t'+j)}=0$ for all $1\leqslant k\leqslant t'$, then we have $\sum_{k=1}^{t} v_k=0$, it follows that $uS=0$, this is a contradiction to $uS\neq 0$. Hence we can assume $1+\sum_{j=1}^{t-t'} g_1'^{(t'+j)}\neq 0$, and set $h^{-1}=1+\sum_{j=1}^{t-t'} g_1'^{(t'+j)}$. Then we have

$$f'^{\psi}=f'^{\psi_1}h+\sum_{j=1}^{t-t'} f'^{\psi_{t'+j}}g_1'^{(t'+j)}h,\ h\in P',$$

$$\psi=\psi_1h_R+\sum_{j=1}^{t-t'} \psi_{t'+j}\,g_{1R}'^{(t'+j)}h_R,\ h_R\in P'_R. \tag{17}$$

It is clear that $\psi_1P'_R+\sum_{j=1}^{t-t'}\psi_{t'+j}P'_R$ is a Galois (P'_R, P'_R)-module. It follows that $\psi-\psi_1h_R-\sum_{j=1}^{t-t'}\psi_{t'+j}g_{1R}'^{(t'+j)}h_R=0$ from (17), hence it is well known that $\psi=\widetilde{\psi}_i\, I_\mu$, where ψ_i is one of $\psi_1, \psi_{t'}\cdots, \psi_t$ and $\mu\in P'$. Let $r^*\in P$, then it follows $r^*I_\mu=r^*$ from $r^{*\psi}=r^*=r^{*\psi_i}$. Hence $\mu\in C_{P'}(P)$.

On the other hand, suppose that $\{u_j\}_{\Gamma'}$ is a P'-base of $\mathfrak{M}$, then $\{u_jS_i\mu_L\}$ is also a P'-base. Hence there exists an element $\omega\in L(P', \mathfrak{M})$ such that $u_jS_i\mu_L\omega=u_jS$, $j\in\Gamma'$. Thus we have $\sum(f'_ju_j)(S_i\mu_L\omega)=\sum(f'_ju_j)S$, hence $S_i\mu_L\omega=S$.

Lemma 3 *Let $\mathfrak{M}=\sum Fu_i$, Φ the center of F. Denote f' an element of F_L. Suppose that $\omega=\sum_{i=1}^{n} f'_i\omega_i$, then there exist elements $\varphi_i\in\Phi$ such that $\omega=\sum_{i=1}^{n}\varphi_i\omega_i$, and suppose that $f'=\sum_{i=1}^{m} f'_i\omega_i$, then there exist $\varphi_i\in\Phi$ such that $f'=\sum_{i=1}^{m} f'_i\varphi_i$, where ω, $\omega_i\in L(F, \mathfrak{M})$, $f'_i\in F_L$.*

Proof First we prove the first assertion. We remark that it is equivalent to prove that if the elements $\omega_1, \cdots, \omega_n$ of $L(F, \mathfrak{M})$ are linearly independent over F_L, then these elements are also linearly indepedent over Φ. Thus we suppose that we have a non-trivial relation $\sum_i g'_i\omega_i=0$ connecting $\omega_1, \cdots, \omega_n$. We may suppose that our relation is a shortest one in the sense that the number of non-zero coefficients is least. Of course, we may suppose that $g'_i\neq 0$. If $\omega_1=0$, it is clear that the $\omega_1, \cdots, \omega_n$ are Φ-dependent. Hence we may assume that $\omega_1\neq 0$ and put $h'_i=g_1'^{-1}g'_i$, then our relation has the form ω_1+

$h'_2\omega_2+\cdots=0$. We may suppose that $h'_2\neq 0$. If f' is any element in F_L, then we have

$$0=f'\omega_1+f'h'_2\omega_2+\cdots=\omega_1 f'+h'_2\omega_2 f'+\cdots.$$

Hence $$(f'h'_2-h'_2 f')\omega_2+\cdots=0.$$

Since the given relation is shortest, $f'h'_2-h'_2f'=0$ holds for all $f'\in F_L$. Thus $h'_2\in\Phi$. In a similar manner we see that all h'_i are in Φ. Hence we have $g'_i=g'_1\varphi_i$, $\varphi_i\in\Phi$. Therefore, we have a non-trivial Φ-relation connecting the ω_i, i.e., $\sum_i \varphi_i\omega_i=0$, $\varphi_i\neq 0$.

Next we prove the second assertion. Suppose that $f'=\sum_{i=1}^{m} f'_i\omega_i$, we shall prove by induction that $f'=\sum_{i=1}^{n} f'_i\varphi_i$, $\varphi_i\in\Phi$. If $m=1$, then it follows obviously from $f'=f'_1\omega_1$, $\omega_1\in L(F, \mathfrak{M})$ that $f'=f'_1\varphi_1$, $\varphi_1\in\Phi$. Suppose that the assertion for $m=k$ is true, we shall show that the assertion for $m=k+1$ is also true. Consider the following relation

$$f'=\sum_{i=1}^{k+1} f'_i\omega_i,\ \omega_i\in L(F, \mathfrak{M}),\ f'_i\in F_L. \tag{18}$$

Of course, we may assume that all $f'_i\omega_i\neq 0$. Then we have

$$\omega_1+f_1'^{-1}f'_2\omega_2+\cdots+f_1'^{-1}f'_{k+1}\omega_{k+1}-f_1'^{-1}f'=0. \tag{19}$$

From the first assertion of our lemma we know there exist $\varphi_i\in\Phi$ such that $\omega_1-\varphi_2\omega_2-\cdots-\varphi_{k+1}\omega_{k+1}-\varphi_1=0$. Now we put this relation into the form (19), hence we have

$$\sum_{j=2}^{k+1}(f'_i\varphi_j+f'_j)\omega_j=f'+f'_1\varphi_1. \tag{20}$$

If $f'+f'_1\varphi_1=0$, it is clear that our assertion is true. Hence we may assume that $f'+f'_1\varphi_1\neq 0$. By induction we know that there exist elements $\tilde{\varphi}_i\in\Phi$, $i=2, \cdots, k+1$ such that

$$f'+f'\varphi_1=\sum_{j=2}^{k+1}(f'_1\varphi_j+f'_j)\tilde{\varphi}_j.$$

Hence $$f'=f'_1\varphi_1^*+\cdots+f'_{k+1}\varphi_{k+1}^*,\ \varphi^*\in\Phi.$$

Theorem 2 *Let $\mathfrak{M}=\sum Fu_i$ be a vector space over a division ring F, G a group of automorphisms of F, G_0 the group of inner automorphisms belonging to G, E' the algebra of G, i.e., $E'=\sum_{I_{r_j}\in G_0}\Phi r_j$, where Φ is the center of F. Let $P'=C_F(E')$, $P=I(G)$. Suppose that $[F:P]_L<\infty$, then we obtain the following results.*

(i) *$C_F(C_F(E'))=E'$; $C_F(P)=E'C_{P'}(P)=C_F(P')C_{P'}(P)$.*

(ii) *$[P':P]_L=[G/G_0]$, where $[G/G_0]$ denotes the index of G_0 in G.*

$[F:P']_L=dim.\ E'=$ the dimension of E' over Φ.

(iii) *if G is Galois, then $C_F(P)=C_F(P')$, and if $S\in L(P,\mathfrak{M})=\sum_{k=1}^{t}\oplus S_kL(P', \mathfrak{M})$ for any P'-semi-linear automorphism S, then there exists an element S_k of $S_1, \cdots, S_t$ such that $SL(P', \mathfrak{M})=S_kL(P', \mathfrak{M})$.*

Proof (i) We prove the first assertion of (i). Let $r\in C_F(P')$, then it follows from theorem 1 that $r_L=\sum_{j=1}^{n} r_{jL}\omega_j$, $\omega_j\in L(F, \mathfrak{M})$, $r_j\in E'$. By lemma 3 there exist elements $\varphi_i\in\Phi$ such that $r_L=\sum_{j=1}^{n} r_{jL}\varphi_j\in E'$. Hence $C_F(P')\subseteq E'\subseteq C_F(P')$.

Now we prove the second assertion of (i). Let $f\in C_F(P)$, then $f_L\in L(P, \mathfrak{M})=\sum_{k=1}^{t}\oplus S_kL(P', \mathfrak{M})$. By lemma 2 we have $f_L=S_k\mu_L\omega'$, $\omega'\in L(P', \mathfrak{M})$, $I_f=\psi_kI_\mu$, $\mu\in C_{P'}(P)$, where ψ_k is the isomorphism associated with S_k. It follows that $I_f I_{\mu^{-1}}=\psi_k\in G$. Hence $f\mu^{-1}\in E'$, $f\in E'\mu$. Thus $C_F(P)\subseteq E'C_{P'}(P)=C_F(P')C_{P'}(P)$. The converse inequality is clear.

Now we prove the first assertion of (ii). By theorem 1 we know that $L(P, \mathfrak{M})=\sum_{k=1}^{t}\oplus S_kL(P', \mathfrak{M})$, $S_k=(S_k, \psi_k)$, $\psi_k\in G$. If there exist two elements S_k and S_j of S_1, $\cdots$, S_t such that their associated isomorphisms ψ_k and ψ_j are in the same cosets modulo G_0, i. e., $\bar{\psi}_k=\bar{\psi}_j\in\bar{G}=G/G_0$, then it follows $\psi_k\psi_j^{-1}\in G_0$, $S_kS_j^{-1}\in L(P', \mathfrak{M})$. This implies that $S_kL(P', \mathfrak{M})=S_jL(P', \mathfrak{M})$, this is contrary to the fact that $\sum_{k=1}^{t} S_kL(P', \mathfrak{M})=\sum_{k=1}^{t}\oplus S_kL(P', \mathfrak{M})$. Hence we have shown that any two isomorphisms ψ_k and ψ_j associated with S_k and S_j respectively, are in different cosets modulo G_0, if S_k and S_j are different elements of $S_1, \cdots, S_t$. It is now clear that $t\leqslant[G/G_0]$. Conversely, if $\bar{\psi}\in G/G_0$, then there exists a P'-semi-linear automorphism $S=(S, \psi)$. By lemma 2 we can obtain $S=S_k\mu_L\omega$, $\psi=\psi_kI_\mu$. But $\psi_k^{-1}\psi\in G$, it follows $I_\mu\in G_0$. Hence $\bar{\psi}_k=\bar{\psi}$. This shows that $[G/G_0]\leqslant t$.

Now we prove the second assertion of (ii). Let $r_{1L}, \cdots, r_{mL}$ be elements of E'_L, then from lemma 3 it follows that $r_{jL}L(F, \mathfrak{M})\cap(\sum_{k\neq j} r_{kL}L(F, \mathfrak{M}))=0$ if and only if $r_{1L}, \cdots, r_{mL}$ are Φ-linearly independent. Thus we can obtain by lemma 1 that $[F:P']_L=\dim. E'$.

(iii) If G is a Galois group, we want to show $C_F(P)=C_F(P')$. In fact, since G is Galois, it follows that the algebra E' of G is $E'=C_F(P)$. From the assertion of (i) it follows $E'=C_F(P')$, therefore, $C_F(P')=C_F(P)$.

Finally we prove the second assertion. By lemma 2 it is clear that $S=S_k\mu_L\omega'$, $\omega'\in L(P', \mathfrak{M})$, $\mu\in C_{P'}(P)$. Since G is Galois, it follows from $C_F(P)=C_F(P')=E'$ that $\mu_L\in L(P', \mathfrak{M})$. Thus $SL(P', \mathfrak{M})=S_kL(P', \mathfrak{M})$.

Now the proof is complete.

The following well known results follow from our theorem 2.

Corollary 4 *Let G be a group of automorphisms of division ring F, $P=I(G)$, assume that $[F:P]_L<\infty$, then G has finite reduced order. In this case $[F:P]_L=$ reduced order of G.*

Proof From theorem 1 and lemma 3 it follows that the first assertion is true. By theorem 2 it is clear that $[F:P]_L=[F:P']_L[P':P]_L=(\dim. E')([G/G_0])$.

Corollary 5 *Let G be an N-group of division ring F, and $[F:I(G)]_L<\infty$, then G is Galois.*

Proof Let $I(G)=P$, and $\widetilde{G}$ be the Galois group of P in F. It is clear that $G\subseteq\widetilde{G}$. Denote G_0, $\widetilde{G}_0$ the groups of inner automorphisms belonging to G and $\widetilde{G}$ respectively, and E', $\widetilde{E}'$ the algebras of G and $\widetilde{G}$ respectively. By theorem 1 and the assertion (iii) of theorem 2, $[G/G_0]\leqslant[\widetilde{G}/\widetilde{G}_0]$.

Since dim. $E'\leqslant$dim. $\widetilde{E}'$, it follows from the corollary 4 of theorem 2 that $[\widetilde{G}/\widetilde{G}_0]\leqslant[G/G_0]$. Hence $[\widetilde{G}/\widetilde{G}_0]=[G/G_0]$. Thus dim. $E'=$dim. $\widetilde{E}'$ and $E'=\widetilde{E}'$. Since G is an N-group, it follows that $G_0=\widetilde{G}_0$. From $G\subseteq\widetilde{G}$ it follows that $G=\widetilde{G}$.

As in the proof of the preceding corollary we can obtain the following theorem:

Theorem 3 (Invariant theorem) *Let F be a division ring, G and G^* be the groups of automorphisms of F, G_0 and G_0^* be the groups of inner automorphisms belonging to G and G^* respectively, let E' and E'^* be the algebras of G and G^* respectively. Suppose that $[F:I(G)]<\infty$, $I(G)=I(G^*)$, then $[G/G_0]=[G^*/G_0^*]$, dim. $E'=$dim. E'^*.*

Lemma 4 *Let F be a division ring, P a division subring of F, let P be Galois in F, and $[F:P]_L<\infty$. Denote G the Galois group of P in F, K a division subring of F and $P\subset K$. Let $[\Theta]$ be the group of F-semi-linear automorphism associated with G. Assume that $[F:K]_L=m$, then $L(K,\mathfrak{M})=\sum_{j=1}^{m}\oplus S_jL(F,\mathfrak{M})=BL(F,\mathfrak{M})$, where $S_j\in B=[\Theta]L(K,\mathfrak{M})$, $T_\nu(K,\mathfrak{M})=BT_\nu(F,\mathfrak{M})$. If $H=\{\psi|S=(S,\psi)\in B\}$, then H is the Galois group of K in F.*

Proof[1] Since $[F:K]_L=m$, we have $F=\sum_{\alpha=1}^{m}Kf^{(\alpha)}$, $\mathfrak{M}=\sum_{\Gamma}Fu_i=\sum_{\substack{\alpha=1,\cdots,m,\\ i\in\Gamma}}Kv_i^{(\alpha)}$, where $v_i^{(\alpha)}=f^{(\alpha)}u_i$. By thorem 1 we know that $L(P,\mathfrak{M})=\sum_{i,j}\oplus S_jr_{ijL}L(F,\mathfrak{M})$, $S_j\in[\Theta]$, $r_{ij}\in E'$. Let $\sigma\in L(K,\mathfrak{M})$ and $\sigma=\sum_{\substack{i=1,\cdots,l\\ j=1,\cdots,m_i}}S_ir_{ijL}\omega_{ij}$, where $S_ir_{ijL}\omega_{ij}\neq0$, put $n=\sum m_i$, then we can prove by induction of n that there exist positive integers $m_i'\leqslant m_i$ and $r'_{ij'}\in E'$ such that $\sigma=\sum_{\substack{i=1,\cdots,l\\ j'=1,\cdots,m_i'}}S_ir'_{ijL}\omega_{ij'}$ and $S_ir'_{ijL}\in L(K,\mathfrak{M})\cap[\Theta]=B$, where $j'=1'$, $\cdots$, m_i', and $1',\cdots,m_i'$ are different numbers of $1,\cdots,m$. In fact, if $n=1$, then the assertion is obviously clear. Now we suppose that the assertion is true for $n=t$, we want to show thatit is also true for $n=t+1$. Since $\sigma\in L(K,\mathfrak{M})$, it follows$(kx)\sigma=k(x\sigma)$ for $k\in K$, $x\in\mathfrak{M}$. Hence we have $\sum_{i,j}(r_{ij}k^{\psi_i}-kr_{ij})(xS_i\omega_{ij})=0$. If $r_{ij}k^{\psi_i}=kr_{ij}$ is true for $i=1,\cdots,l$; $j=1,\cdots,m_i$ and all $k\in K$, then it follows at once that $S_ir_{ijL}\in L(K,\mathfrak{M})$. Therefore, the assertion is true. Conversely, if there exist a pair i_1, j_1 and an element

1) In the first part of our lemma I adopt the proof of my post-graduate student Mr. Huang Changling (黄昌令).

$k_0 \in K$ such that $r_{i_1j_1}k_0^{\psi_{i_1}} - k_0 r_{i_1j_1} \neq 0$, then we have

$$S_{i_1}\omega_{i_1j_1} = \sum_{(i,j)\neq(i_1,j_1)} S_i\omega_{ij}\delta_{ijL}, \tag{21}$$

where $\delta_{ij} = (r_{i_1j_1}k_0^{\psi_{i_1}} - k_0 r_{i_1j_1})^{-1}(r_{ij}k_0^{\psi_i} - k_0 r_{ij})$. Since $S_i\omega_{ij} \in L(P, \mathfrak{M})$, it follows from (21) that $\sum_{(i,j)\neq(i_1,j_1)} (\delta_{ij}p - p\delta_{ij})(xS_i\omega_{ij}) = 0$ for all $p \in P$. If $\delta_{ij} \in C_F(P)$, then $\delta_{ijL} \in L(P', \mathfrak{M})$ by theorem 2 (iii). From $L(P, \mathfrak{M}) = \sum \oplus S_i L(P', \mathfrak{M})$ and by (21) it follows that $S_i\omega_{i_1j_1} = \sum_{j\neq j_1} S_i\omega_{i_1j}\delta_{i_1jL}$. Consequently, by lemma 3, $\omega_{i_1j_1} = \sum_{j\neq j_1} \omega_{ij}\delta_{i_1jL} = \sum_{j\neq j_1} \varphi_j\omega_{i_1j}$, $\varphi_i \in \Phi$. Then we put it into $\sigma = \sum_{\substack{i=1,\dots,l\\ j=1,\dots,m_i}} S_i r_{ijL}\omega_{ij}$, and since G is Galois group of P in F and $r_{i_1j} + \varphi_j r_{i_1j_1} \in E'$, hence we have $(r_{i_1j} + \varphi_j r_{i_1j_1})_L \in [\Theta]$. Thus our assertion is true by the assumption of induction. Hence we may suppose that there exist a pair i_2, j_2 and an element p_2 in P such that $\delta_{i_2j_2}p_2 - p_2\delta_{i_2j_2} \neq 0$, then we can obtain similarly as above

$$S_{i_2}\omega_{i_2j_2} = \sum_{\substack{(i,j)\neq(i_1,j_1)\\ \neq(i_2,j_2)}} S_i\omega_{ij}y_{ijL}. \tag{22}$$

Now by repeating the course of the preceding proof we can show that either the assertion is true or there exist a pair i_3, j_3 and an element p_3 in P such that we have similarly a form as (22), and so on. Finally we may assume that we have the following form:

$$S_{i_q}\omega_{i_qj_q} = S_{i_q'}\omega_{i_q'j_q'}\zeta_L,$$

and therefore $(\zeta p - p\zeta)(xS_{i_q'}\omega_{i_q'j_q'}) = 0$, for all $p \in P$. If there exists an element p_{q+1} such that $\zeta p_{q+1} - p_{q+1}\zeta \neq 0$, then $xS_{i_q'}\omega_{i_q'j_q'} = 0$, hence $\omega_{i_q'j_q'} = 0$, this is a contradiction to $\omega_{i_q'j_q'} \neq 0$. Therefore $\zeta \in C_F(P)$ and we can show that the assertion is true as above. Hence our assertion is true. Thus $L(K, \mathfrak{M}) \subseteq BL(F, \mathfrak{M})$. It is therefore clear that $L(K, \mathfrak{M}) = BL(F, \mathfrak{M})$, where $B = [\Theta] \cap L(K, \mathfrak{M})$. By assumption of H we obtain $K = I(H)$, and clearly H is a group. Let $\tilde{G}$ be the Galois group of K in P, it is clear that $H \subset \tilde{G}$. Denote E' and $\tilde{E}'$ the algebras of G and $\tilde{G}$ respectively, it is clear that $E' \supset \tilde{E}'$. It is obvious that $\tilde{e}'_L \in L(K, \mathfrak{M})$ for any element $\tilde{e}' \in \tilde{E}'$. On the other hand, it follows from the structure of Θ that every element $e' \in E'$ must belong to Θ. It follows that for element $\tilde{e}' \in \tilde{E}$, we have $\tilde{e}'_L \in B = [\Theta] \cap L(K, \mathfrak{M})$. Hence $I\tilde{e}' \in H$. This shows that H is an N-subgroup. By corollary 5 of theorem 2 we know that H is Galois.

Next, since K is Galois in F, then by theorem 1, $L(K, \mathfrak{M}) = \sum_{j=1}^{m} \oplus S'_j L(F, \mathfrak{M})$, where $m = [F:K]_L$. By the preceding proof we know that H is the Galois group and $L(K, \mathfrak{M}) = \sum \oplus S_k L(F, \mathfrak{M})$, $S_k \in B$. Thus we have $m \leqslant l$ from theorem 2 (iii). But by theorem 1, $m \geqslant l$. Therefore $l = m = [F:K]_L$.

Finally we shall show that $T_\nu(K, \mathfrak{M}) = BT_\nu(F, \mathfrak{M})$. In fact, it is clear that $BT_\nu(F, \mathfrak{M}) \subseteq T_\nu(K, \mathfrak{M})$. Now we want to show that the converse inclusion is obvious. As before we can prove that there exists an element $\sigma^* \in L(K, \mathfrak{M})$ for arbitrary m F-

linearly independent elements $y_1, \cdots, y_m$ such that $v_i^{(\alpha)}\sigma^* = y_\alpha$, $\alpha = 1, \cdots, m$. But $\sigma^* = \sum_{j=1}^{m} S_j\omega_j$, $\omega_j \in L(F, \mathfrak{M})$, it is clear that there exists a matrix $(a_{\alpha j})_{m\times m}$ with full rank, where $a_{\alpha j} = f^{(\alpha)\psi_j}$, and $S_j = (S_j, \psi_j)$. Denote σ an element of $T_\nu(K, \mathfrak{M})$ and put $v_i^{(\alpha)}\sigma = \dot{Y}_\alpha(\mathrm{i})$. We consider the system of linear equations $\sum_{j=1}^{m} a_{\alpha j}X_j(\mathrm{i}) = \dot{Y}_\alpha(\mathrm{i})$, $i \in \Gamma$, $\alpha = 1, \cdots, m$. Since $(a_{\alpha j})_{m\times m}$ has full rank, hence the above system has a solution. Hence from $\rho(\sigma) < \aleph_\nu$ it follows that there exist elements $\omega_j' \in T_\nu(F, \mathfrak{M})$ for every j such that $(u_i S_j)\omega_j' = \mathring{X}_j(i)$, $i \in \Gamma$. Put $\bar{\sigma} = \sum_{j=1}^{m} S_j\omega_j'$, then $v_i^{(\alpha)}\sigma = v_i^{(\alpha)}\bar{\sigma}$. Since $\sigma, \bar{\sigma} \in L(K, \mathfrak{M})$, it follows that $\sigma = \bar{\sigma} = \sum S_j T_\nu(F, \mathfrak{M}) \subseteq BT_\nu(F, \mathfrak{M})$. This completes our proof.

Therefore, the following well known finite Galois theory of division rings immediately follows from our corollary 5 of theorem 2 and lamma 4.

Theorem 4 *Let P be Galois in F such that $[F:P]_L$ is finite and let G be the Galois group. Let H be any N-group of G and E any division subring of F containing P. Then the correspondences $H \to I(H)$ and $E \to A(E)$ are inverses of each other.*

References

[1] Yonghua Xu, A theory of rings that are isomorphic to the complete rings of linear transformations (VI) (to appear).

[2] N. Jacobson, Structure of rings, *Amer. Math. Soc. Colloq. Publ.* **37** (1956).

本原环之间的有限结构定理及其在 Galois 理论中的应用

许 永 华
(复旦大学)

摘 要

设 $\mathfrak{M}=\sum Fu_i$ 是除环 F 上向量空间，P 是 F 的一个子除环且在 F 中是 Galois，即存在 F 的一个自同构群 G 使 $I(G)=P$. 记 Φ 是 F 的中心，G_0 是属于 G 的内自同构群，G_0 的元素记为 I_r, $r\in F$. 记 $E'=\sum\limits_{I_{r_j}\in G_0}\Phi r_j$ 是 G 的代数，$P'=C_F(E')$ 是 E' 在 F 中的中心化子. 记 $\mathfrak{L}(F,\ \mathfrak{M})$ 是 $\mathfrak{M}$ 的 F-线性变换完全环，$T_\nu(F,\ \mathfrak{M})$ 是 $\mathfrak{L}(F,\ \mathfrak{M})$ 中所有秩小于 $\aleph_\nu$ 的元素集合，那末我们有如下主要结果：

(1) $[F:P']_L=n$ 有限当且仅当 $T_\nu(P',\ \mathfrak{M})=\sum\limits_{j=1}^{n}\oplus r_{jL}T_\nu(F,\ \mathfrak{M})$，其中 $r_j\in E'$, r_{jL} 表示元素 r_j 的标量左乘.

(2) $[P':P]_L=t$ 有限当且仅当 $T_\nu(P,\ \mathfrak{M})=\sum\limits_{j=1}^{t}\oplus S_jT_\nu(P',\ \mathfrak{M})$，其中 S_j 表示 $\mathfrak{M}$ 的 F-半线变换自同构，它的伴随同构 $\psi_j\in G$.

(3) 如有某个序数 ν 使 $T_\nu(P,\ \mathfrak{M})$, $T_\nu(P',\ \mathfrak{M})$ 及 $T_\nu(F,\ \mathfrak{M})$ 满足(1)及(2)中的关系式，那末对任何 $T_\mu(P,\ \mathfrak{M})$, $T_\mu(P',\ \mathfrak{M})$ 及 $T_\mu(F,\ \mathfrak{M})$ 皆满足(1)及(2)中的关系式. 特别对 $\mathfrak{L}(P,\ \mathfrak{M})$, $\mathfrak{L}(P',\ \mathfrak{M})$ 及 $\mathfrak{L}(F,\ \mathfrak{M})$ 是如此.

(4) 如果 $[F:P]_L$ 有限，那末必有 $C_F(C_F(E'))=E'$, $[F:P']_L=\dim.E'$, $[P':P]_L=[G/G_0]$，其中 $\dim.E'$ 表示 E' 在 Φ 上的维数，$[G/G_0]$ 表示 G_0 在 G 中的指数. 特别 G 是 Galois 群，则 $C_F(P')=C_F(P)=E'$.

(5) 若 $\tilde{G}$ 是 F 的另一自同构群且 $I(G)=I(\tilde{G})$，那末必有 $[G/G_0]=[\tilde{G}/\tilde{G}_0]$, $\dim.E'=\dim.\tilde{E}'$，其中 $\tilde{E}'$ 表示 $\tilde{G}$ 的代数.

如果 P 取为 F 的中心时，于是从上述结果(1)就得出熟知的定理：$[F:\Phi]$ 是有限的当且仅当 $\mathfrak{L}(\Phi,\ \mathfrak{M})=\mathfrak{L}(F,\ \mathfrak{M})\otimes_\Phi F_L$.

另方面，运用我们上述的结果，可导出除环 F 的有限 Galois 理论。