61. *New Foundation of the Theory of Simple Rings.*

By Gorô AZUMAYA.

Mathematical Institute, Nagoya Imperial University.

(Comm. by T. TAKAGI, M.J.A., Dec. 12, 1946.)

Beautiful theory of simple rings and their subrings has been developed mainly by Brauer, Noether and Albert.[1] Jacobson has recently succeeded in obtaining further the Galois theory for quasi fields.[2]

Under a certain new idea we want in the present paper to re-establish and generalize these theories. Our basic method[3] used in the whole consists principally in the fact that if $\mathfrak{N}$ is a simple ring (i. e. a matrix ring over a quasi-field) and $\mathfrak{M}$ a finite $\mathfrak{N}$-module then the $\mathfrak{N}$-endomorphism ring $\mathfrak{N}^*$ of $\mathfrak{M}$ is also simple, $\mathfrak{M}$ is finite with respect to $\mathfrak{N}^*$ and $\mathfrak{N}$ is considered conversely as an $\mathfrak{N}^*$-endomorphism ring of $\mathfrak{M}$; further to every automorphism of $\mathfrak{N}$ there belongs at least one semi-linear transformation of $\mathfrak{M}$. This, together with other related theorems, is discussed in § 1. After these preparations we are able to give in § 2 a quite natural and direct proof to the well-known fundamental theorem for simple rings. In some

[1] See R. Brauer, Über Systeme hyperkomplexer Zahlen, Math. Zeitschr. 30 (1929); E. Neother, Nichtkommutative Algebra, Math. Zeitschr. 39 (1933); M. Deuring, Algebren, Ergebn. Math. 4 (1935); A. A. Albert, Stucture of Algebras, New York (1939).

[2] N. Jacobson, The fundamental theorem of Galois theory for quasi-fields, Ann. Math. 41 (1940).

[3] It is perhaps of some interest to compare our method with those hitherto given. Brauer first used the algebraic closure of coefficient field. Noether built the theory on her beautiful theory of representations in quasi-fields; the difficulties in separability were so removed and the theory was extended from algebras to rings. Embedding the algebra into matrix algebra over the ground field, Weyl and Brauer avoided the representation theory in quasi-fields, though were restricted again to algebras and the theory was not fully expounded; a complete derivation of the theory along this line was given in a note by Kawada-Oi (Zenkoku-Shijô-Sugaku-Danwakai 162). The similar effect was accomplished in Albert's method by forming the direct product with an inverse-isomorphic algebra; a similar approach was given independently also by Chevalley and Nakayama in their seminary in Princeton, as the writer has been informed. Our method is however to characterize the simple ring as a subring of an absolute endomorphism ring (of a certain module). If we restrict ourselves to algebras then our method is more or less similar to those of Weyl-Brauer and Albert. But our absolute endomorphism ring enables us, not only it is much more natural and directer than the matrix ring over the ground field, to built the theory in a far more general case. Indeed Nakayama, to whom also the present work owes useful remarks, has found that our method is particularly of use in his study of "irreducible rings." (The theory will be reported shortly in these proceedings as well as in a joint paper with Nakayama and the writer.)

points, we are led to refined results. The same method enables us moreover, in §3, to extend Jacobson's Galois theory to the case of simple rings to obtain that, given a simple ring $\mathfrak{R}$ and a finite group $\mathfrak{G}$ of its outer automorphisms, there exists a one-to-one correspondence, in the usual manner, between subgroups of $\mathfrak{G}$ and simple subrings of $\mathfrak{R}$ containing all $\mathfrak{G}$-invariant elements of $\mathfrak{R}$.

§1. *Right modul of a simple ring.*

Let $\mathfrak{M}$ be a module. The totality $\mathfrak{A}$ of all endomorphisms of $\mathfrak{M}$ forms an (associative) ring with identity element i. e. the ***absolute endomorphism ring***[4] of $\mathfrak{M}$. Suppose there be given a right operator-ring $\mathfrak{R}$ of $\mathfrak{M}$. Then every right-sided multiplication of element a of $\mathfrak{R}$ induces in $\mathfrak{M}$ an absolute endomorphism $\tilde{a}$ ($\varepsilon\ \mathfrak{A}$) and by means of the mapping $a \rightarrow \tilde{a}$ $\mathfrak{R}$ is homomorphically carried upon a subring $\tilde{\mathfrak{R}}$ of $\mathfrak{A}$. The $\mathfrak{R}$-endomorphism ring of $\mathfrak{M}$ is nothing but the *commuter ring* $V(\tilde{\mathfrak{R}})$ of $\tilde{\mathfrak{R}}$ in $\mathfrak{A}$. Let us say that $\mathfrak{M}$ is *closed with respect to* $\mathfrak{R}$ if $V(V(\tilde{\mathfrak{R}})) = \tilde{\mathfrak{R}}$, that is, if $\tilde{\mathfrak{R}}$ is identical with the $V(\tilde{\mathfrak{R}})$-endomorphism ring, of $\mathfrak{M}$.

Lemma 1. Let $\mathfrak{M}$ *be a (finite or infinite) direct sum of* $\mathfrak{R}$*-submoduli* $\mathfrak{m}_\mu$ $(\mu\, \varepsilon\, M)$ *such that there exists one* $\mathfrak{m}_0$ *to which every* $\mathfrak{m}_\mu$ *is* $\mathfrak{R}$*-homomorphic. If further* $\mathfrak{m}_0$ *is closed with respect to* $\mathfrak{R}$, *then* $\mathfrak{M}$ *is also so.*

Proof. Let $\eta_\mu\, \varepsilon V(\tilde{\mathfrak{R}})$ be, for each $\mu\, \varepsilon\, M$, an extention of an $\mathfrak{R}$-homomorphism between $\mathfrak{m}_0$ and $\mathfrak{m}_\mu$: $\mathfrak{m}_0\eta_\mu = \mathfrak{m}_\mu$, and take in particular η_0 to be idempotent. Then $\eta_0 V(\tilde{\mathfrak{R}})\eta_0$ is, as usual looked upon as an $\mathfrak{R}$-endomorphism ring of $\mathfrak{m}_0$. Consider an arbitrary $V(\tilde{\mathfrak{R}})$-endomorphism α of $\mathfrak{M}: \alpha\ \varepsilon\ V(V(\tilde{\mathfrak{R}}))$. Since $\mathfrak{m}_0\alpha = \mathfrak{M}\eta_0\alpha = \mathfrak{M}\alpha\eta_0 \leqq \mathfrak{m}_0$, α induces in $\mathfrak{m}_0$ an $\eta_0 V(\tilde{\mathfrak{R}})\eta_0$-endomorphism. Hence there exists, by our assumption, an element $a\,\varepsilon\,\mathfrak{R}$ for which $u_0 a = u_0\alpha$ holds for every $u_0\, \varepsilon\, \mathfrak{m}_0$. Further we have $(u_0\eta_\mu)\alpha = (u_0 d)\eta_\mu = (u_0 a)\eta_\mu = (u_0\eta_\mu)a$ for each $\mu\, \varepsilon\, M$ and consequently $\breve{a} = \alpha$. This completes the proof.

Now let $\mathfrak{R}$ be a *simple ring* (with unit element and satisfying the minimum condition for right ideals). Then it is well known that $\mathfrak{R}$ is isomorphic to a matrix ring of a certain dimension, say r, over an up-to-isomorphism uniquely determined quasi-field $\mathfrak{K}$: $\mathfrak{R} \cong (\mathfrak{K})_r$, which we shall call the *quasi-field belonging to (the simple ring)* $\mathfrak{R}$; the matrix degree r is also uniquely determined and shall be denoted by $[\mathfrak{R}]$. Simple right ideals of $\mathfrak{R}$ are all operator-isomorphic and $\mathfrak{R}$ is the direct sum of r simple right ideals. The operator-endomorphism quasi-field $\mathfrak{K}'$ of a simple right ideal $\mathfrak{r}$ is inverse-isomorphic with $\mathfrak{K}$ and $\mathfrak{R}$ is considered conversely as a $\mathfrak{K}'$-endomorphism ring of $\mathfrak{r}$, that is, $\mathfrak{r}$ is closed with respect to $\mathfrak{K}'$.

[4] We consider $\mathfrak{A}$ as a right-hand multiplication domain of $\mathfrak{M}$.

Consider next an $\mathfrak{R}$-right-module $\mathfrak{M}$ on which the unit element of $\mathfrak{R}$ operates as the identity endomorphism. Then $\mathfrak{M}$ is as is well known, the (finite or infinite) direct sum of simple submoduli operator-isomorphic to the simple right ideal $\mathfrak{r}$ of $\mathfrak{R}$. In virtue of Lemma 1, $\mathfrak{M}$ is therefore closed with respect to $\mathfrak{R}$. The (cardinal) number of direct summands is independent of the direct decomposition which we shall denote by $[\mathfrak{M} \mid \mathfrak{R}]$. The behavior of $\mathfrak{M}$, as $\mathfrak{R}$-right-module, is determined by $[\mathfrak{M} \mid \mathfrak{R}]$. If in part cular $[\mathfrak{M} \mid \mathfrak{R}]$ is finite, then $\mathfrak{R}$-endomorphism ring $\mathfrak{R}^*$ of $\mathfrak{M}$ is isomorphic to the $[\mathfrak{M} \mid \mathfrak{R}]$-dimensional matrix ring over $\mathfrak{K}'$ and $[\mathfrak{M} \mid \mathfrak{R}^*] = [\mathfrak{R}]$.[5] These facts we may describe as follows:

Theorem 1. Let $\mathfrak{A}$ be the absolute.endomorphism ring of a module $\mathfrak{M}$ and let there be given a simple subring $\mathfrak{R}$ of $\mathfrak{A}$ containing the identity element of $\mathfrak{A}$. Then:

1) $V(V(\mathfrak{R})) = \mathfrak{R}$.

2) *If $\overline{\mathfrak{R}}$ is a simple subring of $\mathfrak{A}$ isomorphic with $\mathfrak{R}$ such that $[\mathfrak{M} \mid \overline{\mathfrak{R}}] = [\mathfrak{M} \mid \mathfrak{R}]$, then any isomorphism between $\mathfrak{R}$ and $\overline{\mathfrak{R}}$ can be extended to an inner automorphism of $\mathfrak{A}$.*

3) *In case $[\mathfrak{M} \mid \mathfrak{R}]$ is finite, $V(\mathfrak{R})$ is also a simple ring; the quasi-field belonging to it is inverse-isomorphic to that of $\mathfrak{R}$ and moreover*

$$[\mathfrak{M} \mid \mathfrak{R}] = [V(\mathfrak{R})], \quad [\mathfrak{M} \mid V(\mathfrak{R})] = [\mathfrak{R}].$$

As is easy to see, $\mathfrak{M}$ possesses a *(right-) linearly independent basis* over $\mathfrak{R}$ if and only if $[\mathfrak{M} \mid \mathfrak{R}]$ is divisible by $[\mathfrak{R}]$[6] and, if this is the case, the number of elements constituting the basis is equal to $[\mathfrak{M} \mid \mathfrak{R}] / [\mathfrak{R}]$, which we shall call the *(right-sided) rank* of $\mathfrak{M}$ over $\mathfrak{R}$ and denote by $[\mathfrak{M} : \mathfrak{R}]$.

Theorem 2. Let $\mathfrak{M}$, $\mathfrak{A}$, $\mathfrak{R}$ be as in Theorem 1. Given moreover a simple subring $\mathfrak{S}$ of $\mathfrak{R}$ containing the unit element of $\mathfrak{R}$ such that $[\mathfrak{R} \mid \mathfrak{S}]$ is finite. Then:

1) *Any isomorphism φ of $\mathfrak{R}$ into $\mathfrak{A}$ which maps $\mathfrak{S}$ upon itself ($\mathfrak{S}^\varphi = \mathfrak{S}$) can be extended to an inner automorphism of $\mathfrak{A}$.*

2) *When $[\mathfrak{M} \mid \mathfrak{R}]$ is finite, the relation of $V(\mathfrak{S})$ and $V(\mathfrak{R})$ is the same as that of $\mathfrak{R}$ and $\mathfrak{S}$ and there holds $[\mathfrak{R} \mid \mathfrak{S}]\,[V(\mathfrak{R})] = [V(\mathfrak{S}) \mid V(\mathfrak{R})]\,[\mathfrak{S}]$; in particular $\mathfrak{R}$ possesses a right-linearly independent basis aver $\mathfrak{S}$ if and only if $V(\mathfrak{S})$ has the same over $V(\mathfrak{R})$ and we have, in this case, $[\mathfrak{R} : \mathfrak{S}] = [V(\mathfrak{S}) : V(\mathfrak{R})]$.*

Proof. 1) follows readily from Theorem 1, 2), because $[\mathfrak{M} \mid \mathfrak{R}][\mathfrak{r} \mid \mathfrak{S}] =$

[5] For let $1 = e_1 + e_2 + \dots + e_r$ be the decomposition of the unit element 1 of $\mathfrak{R}$ into mutually orthogonal primitive idempotent elements $e_1, e_2, \cdots, e_r$ ($r = [\mathfrak{R}]$). Then $\mathfrak{M} = \mathfrak{M}e_1 + \mathfrak{M}e_2 + \dots + \mathfrak{M}e_r$ and, since $\mathfrak{R}$ is the $\mathfrak{R}^*$-endomorphism ring of $\mathfrak{M}$, each $\mathfrak{M}e_i$ is, as $\mathfrak{R}^*$-module, directly indecomposable. But, since $\mathfrak{R}^*$ is simple and hence every $\mathfrak{R}^*$-module is completely reducible, each $\mathfrak{M}e_i$ is necessarily simple; this implies $[\mathfrak{M} \mid \mathfrak{R}^*] = [\mathfrak{R}]$.

[6] Of course, this is the case when $[\mathfrak{M} \mid \mathfrak{R}]$ is infinite.

$[\mathfrak{M} \mid \mathfrak{S}] = [\mathfrak{M} \mid \mathfrak{R}^{\rho}][\mathfrak{r}^{\rho} \mid \mathfrak{S}]$ and $[\mathfrak{r}^{\rho} \mid \mathfrak{S}]$ is finite, where $\mathfrak{r}$ denotes a simple right ideal of $\mathfrak{R}$.

2) From $[\mathfrak{M} \mid \mathfrak{R}]\,[\mathfrak{r} \mid \mathfrak{S}] = [\mathfrak{M} \mid \mathfrak{S}]$ and $[\mathfrak{R} \mid \mathfrak{S}] = [\mathfrak{R}]\,[\mathfrak{r} \mid \mathfrak{S}]$, it follows $[\mathfrak{R} \mid \mathfrak{S}]\,[\mathfrak{M} \mid \mathfrak{R}] = [\mathfrak{R}]\,[\mathfrak{M} \mid \mathfrak{S}]$. But since $[\mathfrak{M} \mid \mathfrak{S}] = [V(\mathfrak{S})]$ and $[\mathfrak{M} \mid \mathfrak{R}] = [V(\mathfrak{R})]$ by Theorem 1, we have necessarily $[\mathfrak{R} \mid \mathfrak{S}]\,[V(\mathfrak{R})] = [\mathfrak{R}]\,[V(\mathfrak{S})]$. As $[\mathfrak{M} \mid V(\mathfrak{R})] = [\mathfrak{R}]$ whence $[V(\mathfrak{S}) \mid V(\mathfrak{R})]$ is finite, we have, by replacing $\mathfrak{R}$, $\mathfrak{S}$ by $V(\mathfrak{S})$, $V(\mathfrak{R})$ respectively, the similar relation $[V(\mathfrak{S}) \mid V(\mathfrak{R})]\,[\mathfrak{S}] = [V(\mathfrak{S})]\,[\mathfrak{R}]$. Comparison of these two relations gives our desired relation $[\mathfrak{R} \mid \mathfrak{S}]\,[V(\mathfrak{R})] = [V(\mathfrak{S}) \mid V(\mathfrak{R})]\,[\mathfrak{S}]$.

§ 2. *The fundamental theorem for simple rings.*

Theorem 3.[7] *Let $\mathfrak{R}$ be a simple ring with the center Z and let $\mathfrak{S}$ be a simple subalgebra of $\mathfrak{R}$ over Z (such that $[\mathfrak{S} : Z]$ is finite). Then:*

1) *The commuter ring $V_{\mathfrak{R}}(\mathfrak{S})$ of $\mathfrak{S}$ in $\mathfrak{R}$ is also simple and the quasi-field belonging to it is the same as that of the direct product $\mathfrak{R} \times \mathfrak{S}$ (constructed over Z), where $\mathfrak{S}'$ is inverse-isomorphic with $\mathfrak{S}$.*

2) *The commuter ring $V_{\mathfrak{R}}(V_{\mathfrak{R}}(\mathfrak{S}))$ of $V_{\mathfrak{R}}(\mathfrak{S})$ coincides with $\mathfrak{S}$: $V_{\mathfrak{R}}(V_{\mathfrak{R}}(\mathfrak{S})) = \mathfrak{S}$.*[8]

3) *$\mathfrak{R}$ possesses a left- as well as a right- linearly independent basis over $V_{\mathfrak{R}}(\mathfrak{S})$ and the rank of $\mathfrak{R}$ over $V_{\mathfrak{R}}(\mathfrak{S})$ is equal to that of $\mathfrak{S}$ over Z (in both left-and right-hand sides): $[\mathfrak{R} : V_{\mathfrak{R}}(\mathfrak{S})] = [\mathfrak{S} : Z]$*[8]

4) *Any isomorphism φ of $\mathfrak{S}$ into $\mathfrak{R}$ leaving invariant every element of Z can be extended to an inner automorphism of $\mathfrak{R}$.*

5) *The product $\mathfrak{S} \cdot V_{\mathfrak{R}}(\mathfrak{S})$ (constructed inside $\mathfrak{R}$) is direct over the common center $K = \mathfrak{S} \frown V_{\mathfrak{R}}(\mathfrak{S})$ of $\mathfrak{S}$ and $V_{\mathfrak{R}}(\mathfrak{S})$; it coincides moreover with the commuter ring $V_{\mathfrak{R}}(K)$ of K in $\mathfrak{R}$*[8].

Proof. Consider the absolute endomorphism ring $\mathfrak{A}$ of (the module) $\mathfrak{R}$. We may regard $\mathfrak{R}$ as a subring of $\mathfrak{A}$. The operator-endomorphism ring $V(\mathfrak{R}) = \mathfrak{R}$ of the $\mathfrak{R}$-right-module $\mathfrak{R}$ is, the totality of left multiplications of $\mathfrak{R}$ and hence inverse-isomorphic with $\mathfrak{R}$ and $V(\mathfrak{R}') = \mathfrak{R}$. Now $\mathfrak{R} \cdot \mathfrak{R}'$ is, by *Noether-Kurosh's theorem,*[9] *direct* over $Z = \mathfrak{R} \frown \mathfrak{R}'$ and is also simple; moreover $[\mathfrak{R} \mid \mathfrak{S} \times \mathfrak{R}']$

[7] Cf. Noether, l. c. § 5; Deuring, l. c. IV, § 4; Albert, l. c. IV.

[8] These three results were proved hitherto only when $\mathfrak{R}$ is a (finite dimensional) simple algebra over Z.

[9] Neother, l. c. § 4, Erweiterungssatz; Kurosh showed, however, that this Noether's theorem remains still valid in the case when A is a two-sided simple ring with unit element (but not necessarily satisfying the minimum condition for right ideals) and S is even infinite over the center P of A: see A. Kurosh, Direct decompositions of simple rings, Recueil Math. 53 (1942). Under Noether-Kurosh's theorem we shall therefore understand this general form. From this theorem it follows, as is pointed out to me by Nakayama, that if A and S are contained in a certain over-ring in which A and S are element-wise commutative then the product $A \cdot S$ of A and S is direct over P: $A \cdot S = A \times S$; observe that S (whence $A \times S$) need not be two-sided simple.

is finite, because $[\mathfrak{R} \mid \mathfrak{R}_r] = [\mathfrak{R}]$ is so.

Since then $V_{\mathfrak{R}}(\mathfrak{S}) = V(\mathfrak{S}) \frown \mathfrak{R} = V(\mathfrak{S}) \frown V(\mathfrak{R}') = V(\mathfrak{S} \times \mathfrak{R})$, we have our assertion 1) immediately from Theorem 1, 3). Further, Theorem 1, 1) implies $V_{\mathfrak{R}}(V_{\mathfrak{R}}(\mathfrak{S})) = V(V(\mathfrak{S} \times \mathfrak{R}') = (\mathfrak{S} \times \mathfrak{R}') \frown V(\mathfrak{R}) = \mathfrak{S}$; this proves 2). 3) follows from Theorem 2, 2), since every linearly independent basis of $\mathfrak{S}$ over Z is at the same time that of $\mathfrak{S} \times \mathfrak{R}'$ over $\mathfrak{R}'$; the existence of a left basis follows by the left-right symmetry. For 4), φ is uniquely extended, in the natural manner, to an isomorphism between $\mathfrak{S} \times \mathfrak{R}'$ and $\mathfrak{S}^{\varphi} \times \mathfrak{R}'$ leaving invariant every element of $\mathfrak{R}'$. Theorem 2, 1) implies then that there exists a *regular* (=inversible) element c in $V(\mathfrak{R}') = \mathfrak{R}$ such that $c^{-1}xc = x^{\varphi}$ for every $x \varepsilon \mathfrak{S}$. The first half of 5) is also an immediate consequence of the Noether-Kurosh's theorem. The second half follows readily from $[\mathfrak{R}: V_{\mathfrak{R}}(K)][\mathfrak{S} \cdot V_{\mathfrak{R}}(\mathfrak{S}) : V_{\mathfrak{R}}(\mathfrak{S})] = [K:Z][\mathfrak{S}:K] = [\mathfrak{S}:Z] = [\mathfrak{R}: V_{\mathfrak{R}}(\mathfrak{S})]$, according to 3), and $\mathfrak{S} \cdot V_{\mathfrak{R}}(\mathfrak{S}) \leqq V_{\mathfrak{R}}(K)$.

Let now $\mathfrak{R}$ be a *primary* ring (with chain condition). Then $\mathfrak{R}$ is, as is well known, isomorphic with a matrix ring over a completely primary ring and hence for any primitive idempotent element e of $\mathfrak{R}$ the (directly indecomposable) right ideal $e\mathfrak{R}$ is closed with respect to $\mathfrak{R}$. Let us assume furthermore that $\mathfrak{R}$ is *uni-serial*.[10] Then every $\mathfrak{R}$-right-module $\mathfrak{M}$ is, according to the fundamental theorem for uni-serial rings, a direct sum of submoduli all operator-homomorphic to $e\mathfrak{R}$; further if $\mathfrak{M}$ is *faithful* (with respect to $\mathfrak{R}$), then there must appear at least one direct summand which is operator-isomorphic to $e\mathfrak{R}$. These two facts enables us, in virtue of Lemma 1, to generalize Theorem 1, 1) to our uni-serial ring $\mathfrak{R}$. Observing further that the direct product of a normal simple ring and a uni-serial algebra is, on account of the Noether-Kurosh's theorem, also uni-serial,[11] we can prove in the similar way as Theorem 3, 2)

Theorem 3'.[12] *Let $\mathfrak{R}$ be a simple ring with the center Z and let $\mathfrak{S}$ be a uni-serial subalgebra of $\mathfrak{R}$ over Z. Then* $V_{\mathfrak{R}}(V_{\mathfrak{R}}(\mathfrak{S})) = \mathfrak{S}$.

§ 3. *Galois theory for simple rings.*

Let $\mathfrak{R}$ be a simple ring with the center Z and let there be given a *finite*

[10] =Einreihig. See G. Köthe, Verallgemeinerte Abelsche Gruppe mit hyperkomplexem Operatorring, Math. Zeitschr. 39 (1934); K. Asano, Über verallgemeinerte Abelsche Gruppen mit hyperkomplexem Operatorenring und ihre Anwendungen, Jap. Journ. Math. 15 (1939); T. Nakayama, Note on uni-serial and generalized uni-serial rings, Proc. Imp. Acad. Tokyo, 16 (1940).

[11] Because a ring (with unit element and satisfying the minimum conditions for left and right ideals) is uni-serial if and only if every two-sided ideal of it is principal. Cf. Asano l. c. Satz 1, 2 and 13.

[12] Cf. Asano, l. c. Satz 17.

group of its outer automorphisms[(13)] $\mathfrak{G} = \{1, \sigma, \ldots, \tau\}$. Then we can construct, as usual, a *crossed product* $(\mathfrak{R}, \mathfrak{G})$ as follows:

$$(\mathfrak{R}, \mathfrak{G}) = \Sigma_{\sigma\varepsilon\mathfrak{G}}\, u_\sigma \mathfrak{R}, \quad u_\sigma u_\tau = u_{\sigma\tau}, \; x u_\sigma = u_\sigma x^\sigma \; (x \varepsilon \mathfrak{R}),$$

where $u_1, u_\sigma, \ldots\ldots, u_\tau$ are linearly independent over $\mathfrak{R}$. Identifying each $x \varepsilon \mathfrak{R}$ with $u_1 x \varepsilon u_1 \mathfrak{R}$, 1 being the identity automorphism, we may assume that $\mathfrak{R}$ is a subring of $(\mathfrak{R}, \mathfrak{G})$. Now we can readily verify

Lemma 2. 1) Every $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module $(\mathfrak{R}u_\sigma =) u_\sigma \mathfrak{R}$ is simple.

2) $u_\sigma\mathfrak{R}$ and $u_\tau\mathfrak{R}$ are operator-isomorphic, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, if and only if ($\sigma\tau^{-1}$ is inner and hence) $\sigma = \tau$.

Owing to this lemma we have

Theorem 4. 1) $(\mathfrak{R}, \mathfrak{G})$ is a simple ring.

2) Every subring of $(\mathfrak{R}, \mathfrak{G})$ containing $\mathfrak{R}$ is expressed as $(\mathfrak{R}, \mathfrak{H})$ by a suitable subgroup $\mathfrak{H}$ of $\mathfrak{G}$ and hence also simple.

3) The commuter ring of $\mathfrak{R}$ in $(\mathfrak{R}, \mathfrak{G})$ coincides with the center Z of $\mathfrak{R}$.

Proof. Lemma 2 implies that every non-zero $\mathfrak{R}$-$\mathfrak{R}$-two-sided submodule of $(\mathfrak{R}, \mathfrak{G})$ is of the form $(\mathfrak{R}, \mathfrak{H}) = \Sigma_{\sigma\varepsilon\mathfrak{H}}\, u_\sigma \mathfrak{R}$ for a suitable non-empty subset $\mathfrak{H}$ of $\mathfrak{G}$. But $(\mathfrak{R}, \mathfrak{H})$ forms a ring if and only if $\mathfrak{H}$ is closed under multiplication, that is, $\mathfrak{H}$ forms, since $\mathfrak{G}$ is a finite group, a subgroup of $\mathfrak{G}$; while $(\mathfrak{R}, \mathfrak{H})$ forms an ideal of $(\mathfrak{R}, \mathfrak{G})$ if and only if $\mathfrak{H} = \mathfrak{G}$. Thus 2), 1) are proved. For 3), take an arbitrary commuter $\Sigma_{\sigma\varepsilon\mathfrak{G}}\, u_\sigma a_\sigma$ $(a_\sigma \varepsilon \mathfrak{R})$ of $\mathfrak{R}$ in $(\mathfrak{R}, \mathfrak{G})$. Then $\Sigma_\sigma u_\sigma a_\sigma x = x \Sigma_\sigma u_\sigma a_\sigma = \Sigma_\sigma u_\sigma x^\sigma a_\sigma$ whence $a_\sigma x = x^\sigma a_\sigma$ for every $\sigma \varepsilon \mathfrak{G}$ and $x \varepsilon \mathfrak{R}$. The latter equality implies that, if we associate with each $u_\sigma^{-1} x$ the element $a_\sigma x$ we have an operator-homomorphism between $u_\sigma^{-1}\mathfrak{R}$ and $a_0\mathfrak{R}$ for each $\sigma \varepsilon \mathfrak{G}$.. But since every $u_\sigma^{-1}\mathfrak{R}$ is simple by Lemma 2, this homomorphism is necessarily an isomorphism, and $a^\sigma \neq 0$; this implies however that σ is inner whence $= 1$, because $a_\sigma x a_\sigma^{-1} = x^\sigma$ for every $x \varepsilon \mathfrak{R}$, and we have $\Sigma_\sigma u_\sigma a_\sigma = a_1 \varepsilon Z$.[(14)]

Now we prove

Theorem 5. Let $\mathfrak{R}$ be a simple ring and let $\mathfrak{G}$ be a finite group of its outer automorphisms. Then:

1) The $\mathfrak{G}$-invariant subring $\mathfrak{S}$[(15)] of $\mathfrak{R}$ is simple.

2) $\mathfrak{G}$ is the totality of automorphisms of $\mathfrak{R}$ which leave invariant every element of $\mathfrak{S}$.[(16)]

[(13)] We mean that all the automorphisms in $\mathfrak{G}$ except the identity are outer.

[(14)] Above arguments also remain valid when a factor set is introduced.

[(15)] We mean that $\mathfrak{S}$ is the subring consisting of all elements of $\mathfrak{R}$ which remain invariant under every automorphism in $\mathfrak{G}$.

[(16)] This is a somewhat more general assertion than the corresponding Jacobson's result.

3) $\mathfrak{R}$ *possesses a linearly independent basis over* $\mathfrak{S}$ *and has the same rank over* $\mathfrak{R}$ *as the order of* $\mathfrak{G}$ (*on both left-and right-hand sides*): $[\mathfrak{R}:\mathfrak{S}] = (\mathfrak{G}:1)$.[17]

4) *The commuter ring* $V_{\mathfrak{R}}(\mathfrak{S})$ *of* $\mathfrak{S}$ *in* $\mathfrak{R}$ *coincides with the center* Z *of* $\mathfrak{R}$, *and hence the center of* $\mathfrak{S}$ *is* $\mathfrak{S}\ \ Z$.[18]

5) *Every simple subring of* $\mathfrak{R}$ *containing* $\mathfrak{S}$ *is, for a suitable subgroup* $\mathfrak{H}$ *of* $\mathfrak{G}$, *the* $\dot{\mathfrak{H}}$*–invariant subring of* $\mathfrak{R}$.

Proof. Let $\mathfrak{A}$ be, as in the proof of Theorem 3, an absolute endomorphism ring of $\mathfrak{R}$. We may assume then that $\mathfrak{R}$ is a subring of $\mathfrak{A}$; the commuter ring $V(\mathfrak{R}) = \mathfrak{R}'$ of $\mathfrak{R}$ is inverse-isomorphic with $\mathfrak{R}$ and $V(\mathfrak{R}') = \mathfrak{R}$, $\mathfrak{R}$ $\mathfrak{R} = Z$.

Furthermore $\mathfrak{G}$ is naturally looked upon as a group of outer automorphisms of $\mathfrak{R}$ Regarding every automorphism σ in $\mathfrak{G}$ as an absolute endomorphism of $\mathfrak{R}$ we get readily $x\sigma = \sigma x^{\sigma}$ for every $x \varepsilon \mathfrak{R} (\leqq \mathfrak{A})$. Therefore, if we associate with every $\Sigma_{\sigma} u_{\sigma} x_{\sigma} \varepsilon$ $(\mathfrak{R}, \mathfrak{G})$ the element $\Sigma_{\sigma} \sigma x_{\sigma} \varepsilon\, \mathfrak{A}$, we obtain a homomorphism between $(\mathfrak{R}, \mathfrak{G})$ and the subring $\mathfrak{R}\cdot\mathfrak{G} = (\mathfrak{R}, \sigma\mathfrak{R}, \ldots, \tau\mathfrak{R})$ of $\mathfrak{A}$. But since $(\mathfrak{R}, \mathfrak{G})$ is simple by Theorem 4, this homomorphism is necessarily an isomorphism and we may assume $(\mathfrak{R}, \mathfrak{G}) = \mathfrak{R}\cdot\mathfrak{G}$ $(=\mathfrak{R} + \sigma\mathfrak{R} + \ldots + \tau\mathfrak{R})$. Similarly, since $x'\sigma = \sigma(x')^{\sigma}$ for every $\sigma \varepsilon \mathfrak{G}$, $x' \varepsilon \mathfrak{R}'$, we have also $(\mathfrak{R}', \mathfrak{G}) = \mathfrak{R}'\cdot\mathfrak{G}$ (see Jacobson l. c.).

Now, as is readily seen, the $\mathfrak{G}$–invariant subring $\mathfrak{S}$ of $\mathfrak{R}$ is identical with $\mathfrak{R}\frown V(\mathfrak{G}) = V(\mathfrak{R}')\frown V(\mathfrak{G}) = V(\mathfrak{R}', \mathfrak{G})$: $\mathfrak{S} = V(\mathfrak{R}', \mathfrak{G})$. Hence Theorem 1 implies that $\mathfrak{R}$ is simple as well as $V(\mathfrak{S}) = (\mathfrak{R}', \mathfrak{G})$. On the other hand, since $(\mathfrak{R}', \mathfrak{G})$ possesses a linearly independent basis $1, \sigma, \ldots, \tau$ over $\mathfrak{R}'$, $\mathfrak{R} = V(\mathfrak{R}')$ does the same over $\mathfrak{S} = V(\mathfrak{R}', \mathfrak{G})$ and $[\mathfrak{R}:\mathfrak{S}] = [(\mathfrak{R}', \mathfrak{G}): \mathfrak{R}'] = (\mathfrak{G}:1)$ on account of Theorem 2. Take next an arbitrary automorphism ρ of $\mathfrak{R}$ under which every element of $\mathfrak{S}$ remains invariant. Then ρ can be extended, in virtue of Theorem 2, to an inner automorphism $a \rightarrow u^{-1}au$ of $\mathfrak{A}$; since every element of $\mathfrak{S}$ is invariant under ρ, u lies necessarily in $V(\mathfrak{S}) = (\mathfrak{R}', \mathfrak{G})$. From $\mathfrak{R}' = V(\mathfrak{R})$ and $u^{-1}\mathfrak{R}u = \mathfrak{R}$, it follows $u^{-1}\mathfrak{R}'u = \mathfrak{R}'$ i. e. $\mathfrak{R}'u = u\mathfrak{R}'$. $u\mathfrak{R}'$ is therefore a simple $\mathfrak{R}'$-$\mathfrak{R}'$–two-sided submodule of $(\mathfrak{R}', \mathfrak{G})$ and hence, on account of Lemma 2, $u\mathfrak{R}' = u_{\sigma}\mathfrak{R}$ for a suitable $\sigma \varepsilon \mathfrak{G}$. This implies the existence of a regular element $c \varepsilon \mathfrak{R}' = V(\mathfrak{R})$ such that $u = u_{\sigma} c$; consequently we have $\rho = \sigma \varepsilon \mathfrak{G}$. These prove 1), 2) and 3). 4) follows from $V_{\mathfrak{R}}(\mathfrak{S}) = V(\mathfrak{S}) \frown \mathfrak{R} = (\mathfrak{R}', \mathfrak{G}) \frown V(\mathfrak{R}')$ and Theorem 4, 3). As to 5), let $\mathfrak{T}$ be any simple subring of $\mathfrak{R}$ containing $\mathfrak{S}$. Then the commuter ring $V(\mathfrak{T})$ lies between $V(\mathfrak{S}) = (\mathfrak{R}',$

[17] By using this, we can prove moreover the existence of a normal basis of $\mathfrak{R}$ over $\mathfrak{S}$ in the similar way as in T. Nakayama, Normal basis of a quasi-field, Proc. Imp. Acad. Tokyo, 16 (1941).

[18] This is shown in Jacobson, l. c. only in a special case.

$\mathfrak{G}$) and $V(\mathfrak{N}) = \mathfrak{N}'$ and so we have, according to Theorem 4, $V(\mathfrak{T}) = (\mathfrak{N}', \mathfrak{H})$ for a suitable subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Thus $\mathfrak{T} = V(V(\mathfrak{T})) = V(\mathfrak{N}', \mathfrak{H}) = \mathfrak{N}\frown V(\mathfrak{H})$. is the $\mathfrak{H}$-invariant subring of $\mathfrak{N}$.

Remark 1. Since $K = \mathfrak{S}\frown Z$ is the center of $\mathfrak{S}$ by Theorem 5, 4), $\mathfrak{S}\cdot Z$ $(\leqq \mathfrak{N})$ is direct over K and is simple, according to the Noether-Kurosh's theorem. And the subgroup of $\mathfrak{G}$ belonging to it consists obviously of all automorphisms in $\mathfrak{G}$ which leave invariant every element of Z.

Remark 2. Let $\mathfrak{S}_0$ be the quasi-field belonging to $\mathfrak{S}$. Then we may assume that there exists a system of matrix units $\{e_{ij};\ i, j = 1, 2, \ldots, s\}$ ($s = [\mathfrak{S}]$) in $\mathfrak{S}$ such that $\mathfrak{S}_0$ is their commuter ring in $\mathfrak{S}$ whence $\mathfrak{S} = \Sigma\, e_{ij}\, \mathfrak{S}_0$. Let further $\mathfrak{N}_0$ be the commuter ring of $\{e_{ij}\}$ in $\mathfrak{N}$ whence $\mathfrak{N} = \Sigma e_{ij} \mathfrak{N}_0$. Then $\mathfrak{N}_0$ is simple and, since all $e_{ij} (\varepsilon\, \mathfrak{N})$ are $\mathfrak{G}$-invariant, $\mathfrak{G}$ is considered essentially as a group of outer automorphisms of $\mathfrak{N}_0$ and indeed the $\mathfrak{G}$-invariant subring of $\mathfrak{N}_0$ is $\mathfrak{S}_0$.