Journal of the Mathematical Society of Japan Vol. 5, No. 2, July, 1953.

Wedderburn's theorem, weakly normal rings, and the semigroup of ring-classes.

By Tadasi NAKAYAMA

(Received Feb. 2, 1953)

A well-known theorem of Wedderburn asserts that if a central simple finite-dimensional algebra A, over a field, is a subalgebra of an algebra S and if the unit element of A is also a unit element in S, then S is the Kronecker product $A \times V_S(A)$, where $V_S(A)$ denotes the commuter ring of A in S. An interesting generalization of the theorem was recently obtained by Azumaya [1]. It deals with the notion of maximally central algebras, which was introduced formerly by Azumaya and the writer [2] in a narrower sense, in a different context. In the present note we first offer (§1, Theorem 1 and §3, Theorems, 2, 3) a further generalization of that Wedderburn-Azumaya theorem, dealing simply with a ring A possessing an independent finite right-basis over its (not necessarily commutative) subring C. On the other hand, weakly normal (or "galoisien") subrings of a ring have recently been used effectively by Dieudonné [3] and the writer [7], [9], [10] in studying automorphisms and the Galois theory of rings. The innerly weakly normal case is of particular interest in our context, and our theorem can, togetheor with some other propositions, be given a finer formulation in this case (§3). The maximally central case is a further particular case in which the innerly weakly normal subring C is commutative and is contained in (in fact, coincides with) the center of A. For maximally central rings Azumaya defined the notion of algebra- or ring-classes and introduced their group, a generalization of the Brauer group of the classes of central simple algebras. We are led to introduce the semigroup of the ring-classes of rings containing a fixed commutative ring C in their center and weakly normal over C (as we want to call) (5). It turns out that Azumaya's group is in fact the largest subgroup in this semigroup (Theorem 5). In Appendix we give a simple proof to Jacobson's inverse to Wedderburn's theorem.

The writer wishes to thank G. Azumaya for his kind cooperation during the preparation of the present paper.

§ 1. Endomorphism rings over subrings.

Let A be, throughout the present note, an (associative) ring with unit element 1. Let C be a subring of A. We assume always that C contains the unit element 1 of A and moreover A possesses an independent finite right-basis over C, of rank n, say;[1]

$$A = a_1 C \oplus a_2 C \oplus \cdots \oplus a_n C.$$

Let $\mathfrak{A}$ be the absolute endomorphism ring of A as a modul. With a subset X of A we denote by X_R (resp. X_L) the set of right (resp. left) multiplications of the elements of X onto A, which we consider as a subset of $\mathfrak{A}$. The C-right-endomorphism ring of A is nothing but the commuter ring $V_{\mathfrak{A}}(C_R)$ of C_R in $\mathfrak{A}$. $V_{\mathfrak{A}}(C_R)$ contains the left-multiplication ring A_L of A and possesses, as follows from our assumption, an independent right-basis of rank n over A_L;

$$V_{\mathfrak{A}}(C_R) = \gamma_1 A_L \oplus \gamma_2 A_L \oplus \cdots \oplus \gamma_n A_L.$$

In fact, $V_{\mathfrak{A}}(C_R)$ is $V_{\mathfrak{A}}(C_R)$-right-isomorphic to the direct sum A^n of n copies of the $V_{\mathfrak{A}}(C_R)$-module A. A further different interpretation of $V_{\mathfrak{A}}(C_R)$ is that it is the relation-module with respect to 1×1 of the A-double-module $A +_C A$, in the sense of [8] e.g. We note also that $V_{\mathfrak{A}}(V_{\mathfrak{A}}(C_R)) = C_R$.

PROPOSITION 1. *Let $\gamma_1, \gamma_2, \cdots, \gamma_m$ be a finite set of elements in the absolute endomorphism ring $\mathfrak{A}$ of A such that the sum*[2] *$\gamma_1 A_L + \gamma_2 A_L + \cdots + \gamma_m A_L$ forms a ring. In order that $\gamma_1 A_L + \gamma_2 A_L + \cdots + \gamma_m A_L$ is $V_{\mathfrak{A}}(C_R)$ with a certain subring $C\,(\ni 1)$ of A over which A possesses an independent right-basis and $\gamma_1, \gamma_2, \cdots, \gamma_m$ are right-independent over A_L, it is necessary and sufficient that there exist m elements $x_1, x_2, \cdots, x_m$ in A such that the matrix*

1) Thus, if C satisfies the minimum (maximum) condition for right-ideals, then A satisfies the same (for C-right-modules, whence) for right-ideals. On the other hand, if A satisfies the left minimum (maximum) condition, then C satisfies the same; consider $a_1\mathfrak{l} \oplus a_2\mathfrak{l} \oplus \cdots \oplus a_n\mathfrak{l}$ with left-ideals $\mathfrak{l}$ of C.

2) Not necessarily direct, for the moment.

$$(x_j^{\gamma_i})=\begin{pmatrix} x_1^{\gamma_1} & \cdots & x_m^{\gamma_1} \\ & \cdots\cdots & \\ x_1^{\gamma_m} & \cdots & x_m^{\gamma_m} \end{pmatrix}$$

in A is regular. If this is the case the m elements $x_1, x_2, \cdots, x_m$ form an independent right-basis of A over C.

PROOF. Suppose, firstly, that $\gamma_1, \gamma_2, \cdots, \gamma_m$ are right-independent over A_L and that $\gamma_1 A_L \oplus \cdots \oplus \gamma_m A_J = V_{\mathfrak{A}}(C_R)$ with a subring $C \ni 1$, of A, over which A possesses an independent right-basis $(a_1, a_2, \cdots, a_n)$, of rank n. Then[3] $V_{\mathfrak{A}}(C_R) = \alpha_1 A_L \oplus \cdots \oplus \alpha_n A_L$ with $\alpha_i \in V_{\mathfrak{A}}(C_R)$ defined by

$$a_j^{\alpha_i} = \delta_{ij} \qquad \text{(Kronecker's } \delta).$$

Thus necessarily[4] $m=n$ and there exists a regular matrix $\big((b_{ij})_L\big)$ of degree n in A_L such that

$$(\gamma_1, \gamma_2, \cdots, \gamma_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)\,\big((b_{ij})_L\big)\,.$$

Setting $x_j = a_j$ we have

$$(x_j^{\gamma_i})_{ij} = (a_j^{\gamma_i})_{ij} = (\textstyle\sum_k b_{ki}\, a_j^{\alpha_k}) = (b_{ji})_{ij}\,.$$

Since the matrix $\big((b_{ij})_L\big)$ in A_L is regular, the matrix $(b_{ji})_{ij}$ in A is regular, and the first half of our proposition is proved.

Assume, conversely, that $(x_j^{\gamma_i})$, with a certain set $x_1, x_2, \cdots, x_m$ of elements in A, possesses an inverse $(d_{ij})_{ij}$. Putting $\delta_i = \sum_k \gamma_k (d_{ik})_L$, we obtain $(x_j^{\delta_i}) = (d_{ij})(x_j^{\gamma_i}) = I$, the unit n-matrix in A. So we see readily that we may assume that $(x_j^{\gamma_i}) = I$ from the beginning. It is then evident that such $\gamma_1, \gamma_2, \cdots, \gamma_m$ are right-independent over A_L. For an arbitrary element $\alpha = \gamma_1 z_{1L} + \gamma_2 z_{2L} + \cdots + \gamma_m z_{mL}$ in $\sum \gamma_i A_L$ we have $x_j^\alpha = z_j$, or $\alpha = \gamma_1 (x_1^\alpha)_L + \gamma_2 (x_2^\alpha)_L + \cdots + \gamma_m (x_m^\alpha)_L$. With $\beta \in \sum \gamma_i A_L$ and $y \in A$, set $\alpha = \gamma_h y_L \beta$. Then, by the above observation,

$$\alpha = \gamma_h y_L \beta = \sum \gamma_i\, (x_i^{\gamma_h y_L \beta})_L = \sum \gamma_i\, (\delta_{ih} y^\beta)_L = \gamma_h (y^\beta)_L\,.$$

Thus $\gamma_h y_L \beta = \gamma_h (y^\beta)_L$ and

3) Cf. [8] for instance. If m is infinite, then we have merely the inclusion that the left-hand side contains the right-hand side. But we see immediately that n is equal to m and is finite.

4) Take for instance, a maximal right-ideal $\mathfrak{m}$ of A_L and consider the fully reducible A_L-right-module $V_{\mathfrak{A}}(C_R)/V_{\mathfrak{A}}(C_R)\,\mathfrak{m}$.

$$(y\, z^{\gamma_h})^{\beta} = y^{\beta}\, z^{\gamma_h}$$

for every $z \in A$. Since β is arbitrary in $\sum \gamma_i A_L$, this shows that

$$(z^{\gamma_h})_R \in V_{\mathfrak{A}}(\sum \gamma_i A_L),$$

for every $z \in A$. Put $V_{\mathfrak{A}}(\sum \gamma_i A_L) = C_R$, with a subring C of A. Our elements $x_1, x_2, \cdots, x_m$ are right-independent over C. For, if $x_1 c_1 + x_2 c_2 + \cdots + x_m c_m = 0$ with $c_i \in C$, then $c_i = \sum \delta_{ij} c_j = \sum x_j^{\gamma_i} c_j = \sum x_j c_j^{\gamma_i} = 0^{\gamma_i} = 0$. Moreover, for an arbitrary element z in A we have $z^{\gamma_i} \in C$, as was seen above. Putting $z' = x_1 z^{\gamma_1} + x_2 z^{\gamma_2} + \cdots + x_m z^{\gamma_m}$, we get $(z'-z)^{\gamma_i} = 0$, for $i = 1, 2, \cdots, m$. Thus $(z'-z)^{\gamma} = 0$ for every $\gamma \in \sum \gamma_i A_L$. In particular, $(z'-z)^{A_L} = A(z'-z) = 0$, and $z'-z = 0$. This shows that $z \in x_1 C + x_2 C + \cdots + x_m C$. Hence $x_1, x_2, \cdots, x_m$ form an independent right-basis of A over C. Clearly $V_{\mathfrak{A}}(C_R) \geqq \sum \gamma_i A_L$. But it is easy to see, from $(x_j^{\gamma_i}) = I$, that here $V_{\mathfrak{A}}(C_R) = \sum \gamma_i A_L$. The proposition is thus proved.

PROPOSITION 2. *Let A possess an independent finite right-basis over C. Then $V_{\mathfrak{A}}(C_R)$-allowable submodules $\mathfrak{a}$ of A are in $1-1$ correspondence with left-ideals $\mathfrak{l}$ of C, according to the correspondence*

$$\mathfrak{a} \rightarrow \mathfrak{l} = C \frown \mathfrak{a}, \qquad \mathfrak{l} \rightarrow \mathfrak{a} = A\,\mathfrak{l}.$$

PROOF. Let $(a_1, a_2, \cdots, a_n)$ be an independent C-right-basis of A, and let $\alpha_i \left(\in V_{\mathfrak{A}}(C_R)\right)$ be such that $a_j^{\alpha_i} = \delta_{ij}$. Let $\mathfrak{a}$ be a $V_{\mathfrak{A}}(C_R)$-allowable submodule of A. If $a \in \mathfrak{a}$ and $a = a_1 c_1 + a_2 c_2 + \cdots + a_u c_n$ $(c_i \in C)$, then

$$a^{\alpha_i} = a_1^{\alpha_i} c_1 + a_2^{\alpha_i} c_2 + \cdots + a_n^{\alpha_i} c_n = c_i\,.$$

Since $a^{\alpha_i} \in \mathfrak{a}$, we have $c_i\,(= a^{\alpha_i}) \in \mathfrak{a} \frown C$. This shows that $\mathfrak{a} \leqq a_1 \mathfrak{l} \oplus a_2 \mathfrak{l} \oplus \cdots \oplus a_n \mathfrak{l} = A\,\mathfrak{l}$ with $\mathfrak{l} = \mathfrak{a} \frown C$. As $\mathfrak{l} \leqq \mathfrak{a}$, clearly $A\,\mathfrak{l} = \mathfrak{l}^{A_L} \leqq \mathfrak{a}$ too. Hence $\mathfrak{a} = A\,\mathfrak{l}$. Here $\mathfrak{l} = \mathfrak{a} \frown C$ is a left-ideal of C, since both $\mathfrak{a}$, C are C_L-allowable.

Let, conversely, $\mathfrak{l}$ be an arbitrary left-ideal of C. Set $\mathfrak{a} = A\,\mathfrak{l}$. For every $\alpha \in V_{\mathfrak{A}}(C_R)$ we have $\mathfrak{a}^{\alpha} = A^{\alpha}\,\mathfrak{l} \leqq A\,\mathfrak{l} = \mathfrak{a}$, and $\mathfrak{a}$ is a $V_{\mathfrak{A}}(C_R)$-allowable submodule of A. Hence, by our above consideration, $\mathfrak{a} = a_1(\mathfrak{a} \frown C) \oplus a_2(\mathfrak{a} \frown C) \oplus \cdots \oplus a_n(\mathfrak{a} \frown C)$. On the other hand, clearly $\mathfrak{a} = A\,\mathfrak{l} = a_1 \mathfrak{l} \oplus a_2 \mathfrak{l} \oplus \cdots \oplus a_n \mathfrak{l}$. Since $a_1, a_2, \cdots, a_n$ are right-independent, we have $\mathfrak{l} = \mathfrak{a} \frown C$. The proposition is thus proved.

THEOREM 1. *Let A possess an independent finite right-basis over its subring C. Let M be a finitely generated right-module of $V_{\mathfrak{A}}(C_R)$,* *possessing the unit element* $1_L\,(=1_R)$ *of* $V_{\mathfrak{A}}(C_R)$ *as an identity operator. Let* M_0 *be the totality of elements* w *in* M *such that*

$$(w\,x_L)^\alpha = w\,(x^\alpha)_L$$

for every $x \in A$ *and* $\alpha \in V_{\mathfrak{A}}(C_R)$. *Then* M *is, considered as an* A_L $\left(\leq V_{\mathfrak{A}}(C_R)\right)$*-right-module, the Kronecker product, over* C_L*, of the* C_L*-right-module* M_0 *and the* C_L*-*A_L*-module* A_L.

PROOF. We have $M = v_1 V_{\mathfrak{A}}(C_R) + v_2 V_{\mathfrak{A}}(C_R) + \cdots + v_s V_{\mathfrak{A}}(C_R)$ with some elements $v_1, v_2, \cdots, v_s$ of M. Each $V_{\mathfrak{A}}(C_R)$-right-module $v_t V_{\mathfrak{A}}(C_R)$ is a homomorphic image of $V_{\mathfrak{A}}(C_R)$, while $V_{\mathfrak{A}}(C_R)$ is, as a $V_{\mathfrak{A}}(C_R)$-module, isomorphic to the direct sum A^n of n copies of A, n being the C-right-rank of A as before. Thus M is a sum of some $\left(V_{\mathfrak{A}}(C_R)\right)$-submodules which are homomorphic images of A. Set thus

$$M = A^{\varphi_1} + A^{\varphi_2} + \cdots + A^{\varphi_h}$$

with $V_{\mathfrak{A}}(C_R)$-homomorphic mappings φ_k of A onto submodules A^{φ_k} of M.

Let M_0 be the submodule of M defined in our theorem. It is a C_L-right-module. For, if $w \in M_0$ and $c \in C$, then

$$(w\,c_L\,x_L)^\alpha = \left(w\,(x\,c)_L\right)^\alpha = w\left((x\,c)^\alpha\right)_L = w\,(x^\alpha\,c)_L = w\,c\,(x^\alpha)_L$$

for every $x \in A$. Further, for each i, C^{φ_i} is contained in M_0. For, if $c \in C$, we have, on putting $\varphi = \varphi_i$,

$$(c^\varphi\,x_L)^\alpha = \left((c^{x_L})^\varphi\right)^\alpha = (x\,c)^{\varphi\alpha} = (x\,c)^{\alpha\varphi} = (x^\alpha\,c)^\varphi = c\,(x^\alpha)_L{}^\varphi = c^\varphi(x^\alpha)_L\,.$$

Since $A^{\varphi_i} = (A\,C)^{\varphi_i} = C^{A_L\varphi_i} = C^{\varphi_i}A_L$, we have

$$M = M_0\,A_L = M_0\,a_{1L} + M_0\,a_{2L} + \cdots + M_0\,a_{nL}\,,$$

where $(a_1, a_2, \cdots, a_n)$ is an independent C-right-basis of A $\left(\text{whence } (a_{1L}, a_{2L}, \cdots, a_{nL})\right.$ is an independent C_L-left-basis of $\left.A_L\right)$. Moreover, if $w_1\,a_{1L} + w_2\,a_{2L} + \cdots + w_n\,a_{nL} = 0$ with some $w_1, w_2, \cdots, w_n \in M$, then

$$w\,(a_1^\alpha)_L + w_2\,(a_2^\alpha)_L + \cdots + w_n\,(a_n^\alpha)_L = 0^\alpha = 0\,.$$

On setting $\alpha = \alpha_i$ (with $a_j^{\alpha_i} = \delta_{ij}\,a_i$), we have

$$w_i\,1_L = 0\,, \qquad \text{or,} \qquad w_i = 0\,.$$

This shows that $a_{1L}, a_{2L}, \cdots, a_{nL}$ are M_0-left-independent, and $M = M_0 \times_{C_L} A_L$.

Remark. As $(w x_L) y_L = w(x_L y_L) = w(y x)_L = w(x^{y_L})_L$ for every $w \in M$ and $x, y \in A$, our M_0 is characterized also as the totality of elements w in M such that

$$(w x_L) \gamma_i = w (x^{\gamma_i})_L \qquad (i = 1, 2, \cdots, n),$$

where $A_{\mathfrak{A}}(C_R) = \sum \gamma_i A_L$.

§ 2. Weakly normal rings.

Let A, C be as in § 1. If then an independent right-basis $\gamma_1, \gamma_2, \cdots, \gamma_n$ of $V_{\mathfrak{A}}(C_R)$ over A_L can be so taken as each γ_i is an A_L-semilinear endomorphism of A, belonging to a (ring)-automorphism θ_i of A, we say that C is a *weakly normal subring* of A and that A is *weakly normal over C.*

PROPOSITION 3. *A is weakly normal over C if and only if the Kronecker product $A \times_C A$ over C is a direct sum*

$$A \times_C A = u_1 A \oplus u_2 A \oplus \cdots \oplus u_n A,$$

where $u_1, u_2, \cdots, u_n$ are A-(right-, say) independent over A and satisfy

$$a u_i = u_i a^{\tau_i} \qquad (a \in A)$$

with some automorphisms $\tau_1, \tau_2, \cdots, \tau_n$ of A. In fact, if this is the case, we can choose A_L-semilinear endomorphisms $\gamma_1, \gamma_2, \cdots, \gamma_n$ of A forming an independent (right-) basis of $V_{\mathfrak{A}}(C_R)$ over A_L so that they belong to the automorphisms $\theta_1, \theta_2, \cdots, \theta_n$ of A_L given by

$$(a_L)^{\theta_i} = (a^{\tau_i})_L,$$

and conversely.

PROOF. We repeat our proof in [9], for the sake of completeness. Assume first that A is weakly normal over C and let γ_i, θ_i be as above. Since $V_{\mathfrak{A}}(C_R) = \gamma_1 A_L \oplus \gamma_2 A_L \oplus \cdots \oplus \gamma_n A_L$ is the relation-module of the A-double-module $A \times_C A$ with respect to $u_0 = 1 \times 1$, it follows (cf. [8]) that there exists an independent A-right-basis $(u_1, u_2, \cdots, u_n)$ of $A \times_C A$ such that

$$x\,u_0=\sum u_i\,x^{\gamma_i} \qquad (x \in A).$$

Define the automorphisms τ_i of A by means of the automorphisms θ_i of A_L as is indicated in our proposition. We have $\sum u_i\,(a\,x)^{\gamma_i}=\sum u_i\,a^{\tau_i}\,x^{\gamma_i}$. The left-hand side is equal to $a\,x\,u_0=\sum a\,u_i\,x^{\gamma_i}=\sum u_j\,\rho_{ji}\,(a)\,x^{\gamma_i}$, where we set $a\,u_i=\sum u_j\,\rho_{ji}\,(a)$ $(\rho_{ji}\,(a) \in A)$. Thus $a^{\tau_j}\,x^{\gamma_j}=\sum \rho_{ji}\,(a)\,x^{\gamma_i}$, whence $\gamma_j\,a_L^{\theta_j}=\sum \gamma_i\,\rho_{ji}\,(a)_L$. Since $\gamma_1, \gamma_2, \cdots, \gamma_n$ are independent over A_L, we have $\rho_{ji}\,(a)_L=\delta_{ji}\,a_L^{\theta_j}$, or $\rho_{ji}\,(a)=\delta_{ji}\,a^{\tau_j}$. Hence $a\,u_i=u_i\,a^{\tau_i}$, which proves a one-half of our proposition.

To prove the other half, assume the existence of an independent right-basis $(u_1, u_2, \cdots, u_n)$ of $A \times_C A$ over A satisfying our condition. The relation-module $V_{\mathfrak{A}}\,(C_R)$ of $A \times_C A$ with respect to $u_0=1\times 1$ has a form $\sum \gamma_i\,A_L$ with γ_i satisfying $x\,u_0=\sum u_i\,x^{\gamma_i}$ $(x \in A)$. Here $\gamma_1, \gamma_2, \cdots, \gamma_n$ are right-independent over A_L, because $A \times_C A$ has an independent right-basis over A contained in $A\,u_0=A\times 1$, derived from an independent right-basis of A over C; cf. [8]. We have $a\,x\,u_0=\sum u_i\,(a\,x)^{\gamma_i}$. But also $a\,x\,u_0=a\sum u_i\,x^{\gamma_i}=\sum u_i\,a^{\gamma_i}\,x^{\gamma_i}$. Hence $(a\,x)^{\gamma_i}=a^{\tau_i}\,x^{\gamma_i}$ and $a_L\,\gamma_i=\gamma_i\,a_L^{\theta_i}$. Thus A is weakly normal over C, which completes our proof.

Remark. The set $\{\theta_1, \theta_2, \cdots, \theta_n\}$ of automorphisms of A_L (or the set $\{\tau_1, \tau_2, \cdots, \tau_n\}$ of automorphisms of A (as in Proposition 3)) is not at all unique, in general. But it is unique up to inner automorphisms, provided that A satisfies the double chain condition for two-sided ideals (or any other condition which makes the Krull-Remak-Schmidt theorem applicable to the A double-module $A \times_C A=\sum u_i\,A$).

PROPOSITION 4. *Let A be weakly normal over its subring C. If, and only if, C satisfies the right (left) minimum condition, A satisfies the right (left) minimum condition, and if, moreover, C is semisimple (resp. simple), then A is semisimple (resp. semisimple with mutually isomorphic simple components).*

PROOF. We have $V_{\mathfrak{A}}\,(C_R)=\sum_{i=1}^{n} \gamma_i\,A_L=\sum A_L\,\gamma_i$ with A_L-semilinear endomorphisms γ_i of A. On the other hand, $V_{\mathfrak{A}}\,(C_R)$ is a matric ring, of degree n, over a ring inversely isomorphic to C. If A satisfies the right (left) minimum condition then $V_{\mathfrak{A}}\,(C_R)$ satisfies the minimum condition for its A_L-left (right) submodules, hence much the more the left (right) minimum condition. Then we have the left (right) minimum condition in the ring inversely isomorphic to C, whence the right (left) minimum condition in C. (The left minimum condition assertion is indeed an immediate consequence of Proposition 2 and may also be treated directly by considering $\sum a_i \mathfrak{l}$ for left ideals $\mathfrak{l}$ in C (where (a_i) is an independent C-right-basis of A)[5]). It is clear,[6] on the other hand, that the right minimum condition in C implies the same condition in A. Further, the left minimum condition in C implies the right minimum condition in $V_{\mathfrak{A}}(C_R)$, which in turn implies the right minimum condition in A_L (or the left minimum condition in A); observe that if $\mathfrak{l}_L$ is a right ideal in A_L then $\sum \mathfrak{l}_L \gamma_i$ is a right ideal in $V_{\mathfrak{A}}(C_R)$. Let N be the radical of A. Then $\sum \gamma_i N_L$ is contained in the radical of $V_{\mathfrak{A}}(C_R)$. But, if C is semisimple, then $V_{\mathfrak{A}}(C_R)$ is semisimple too, whence $\sum \gamma_i N_L=0$ and we have $N=0$. Take, then, a simple component of A and construct the sum A_0 of all the simple components which are isomorphic to the chosen one. This sum A_0 is a two-sided ideal of A invariant under any automorphism of A, and we see readily that $\sum \gamma_i A_{0L}$ is a two-sided ideal in $V_{\mathfrak{A}}(C_R)$. If, on the other hand, C is simple, then $V_{\mathfrak{A}}(C_R)$ is so too. Thus $\sum \gamma_i A_{0L}=V_{\mathfrak{A}}(C_R)$, whence $A_0=A$, then.

Remark. Minimum conditions may be replaced by maximum conditions throughout in the first half of our Proposition 4. Further, that the semisimplicity of C implies the semisimplicity of A, in Proposition 4, is valid generally, without the assumption of minimum condition, semisimplicity being understood in the sense of Jacobson [4]. For, we have generally, besides that a matric ring (of finite degree) over a semisimple ring is semisimple, that[7] $\sum \gamma_i N_L$ is contained in the radical of $V_{\mathfrak{A}}(C_R)=\sum \gamma_i A_L$.

§ 3. Innerly weakly normal rings.

If A is weakly normal over its subring C and if the A_L-semilinear endomorphisms $\gamma_1, \gamma_2, \cdots, \gamma_n$ of A, forming an independent A_L-right-basis of $V_{\mathfrak{A}}(C_R)$, can be so chosen that the belonging automorphisms $\theta_1, \theta_2, \cdots,$

5) And has been mentioned in the footnote 1) too.
6) Cf. again the footnote 1).
7) This I owe to Azumaya.

θ_n of A_L are inner automorphisms[8] (i.e. the automorphisms $\tau_1, \tau_2, \cdots, \tau_n$ of A, as in Proposition 3, are inner automorphisms), then we say that A is *innerly weakly normal* over C. In this case, we can choose our elements $\gamma_1, \gamma_2, \cdots, \gamma_n$ of $V_{\mathfrak{A}}(C_R)$, forming an independent A_L-right-basis of $V_{\mathfrak{A}}(C_R)$, so as they are A_L-linear, i.e. $\theta_1=\theta_2=\cdots=\theta_n=1$ (identity automorphisms of A); multiply the original $\gamma_1, \gamma_2, \cdots, \gamma_n$ by some regular elements (inverse to the regular elements effecting the (original) inner automorphisms $\theta_1, \theta_2, \cdots, \theta_n$). Then $\gamma_i \in V_{\mathfrak{A}}(A_L)=A_R$ and $\gamma_i=k_{iR}$ with $k_i \in A$. Let K be the module generated by $k_1, k_2, \cdots, k_n$ over the center Z of A. We have thus

$$V_{\mathfrak{A}}(C_R)=\sum \gamma_i A_L=K_R A_L.$$

The product $K_R A_L$ is the Kronecker product over $Z_R(=Z_L)$, since $k_{1R}, k_{2R}, \cdots, k_{nR}$ are independent over A_L. Further, $C_R=V_{\mathfrak{A}}(V_{\mathfrak{A}}(C_R))=V_{\mathfrak{A}}(K_R A_L)=V_{\mathfrak{A}}(K_R)\frown A_R=V_{A_R}(K_R)$, or

$$C=V_A(K).$$

We have moreover[9] $K_R=A_R\frown K_R A_L=A_R\frown V_{\mathfrak{A}}(C_R)=V_{A_R}(C_R)$, or

$$K=V_A(C).$$

In particular, K is a *ring* which possesses $(k_1, k_2, \cdots, k_n)$ as an independent basis over Z.

PROPOSITION 5. *Let C be a subring of A such that $C=V_A(V_A(C))$. In order that A is innerly weakly normal over C, it is necessary and sufficient that there exist a finite set of elements $k_1, k_2, \cdots, k_n$ in $V_A(C)$ such that $k_1 Z+k_2 Z+\cdots+k_n Z$ is a ring, where Z is the center of A, and that the matrix*

$$(a_j k_i)=\begin{pmatrix} a_1 k_1 & \cdots & a_n k_1 \\ & \cdots\cdots\cdots & \\ a_1 k_n & \cdots & a_n k_n \end{pmatrix}$$

8) If this is the case, then any other set of A_L-semilinear endomorphisms of A forming an independent A_L-right-basis of $V_{\mathfrak{A}}(C_R)$ consists of those belonging to inner automorphisms of A, provided that A satisfies the double chain condition for two-sided ideals, for instance.

9) Express each element of $K_R A_L$ as a linear combination of $k_{1R}, k_{2R}, \cdots, k_{nR}$ with coefficients from A_L, and observe that if it is ($\in A_R$ whence) commutative with all elements of A_L then the coefficients must be in the center $Z_L=Z_R$ of A_L.

with suitable n elements $a_1, a_2, \cdots, a_n$ in A is regular.

PROOF. We get the sufficiency from Proposition 1 on putting $\gamma_i = k_{iR}$. The necessity follows from the same proposition combined with the above consideration.

PROPOSITION 6. *Let A be innerly weakly normal over C, and let K be the commuter $V_A(C)$ of C in A. Then, A-left and K-right-submodules $\mathfrak{a}$ of A are in $1-1$ correspondence with left-ideals $\mathfrak{l}$ of C according to the correspondence*

$$\mathfrak{a} \rightarrow \mathfrak{l} = C \frown \mathfrak{a}, \qquad \mathfrak{l} \rightarrow \mathfrak{a} = A\,\mathfrak{l}.$$

PROOF. As $V_{\mathfrak{A}}(C_R) = K_R A_L$. the assertion follows from Proposition 2.

THEOREM 2. *Let A be innerly weakly normal over C, and let $K = V_A(C)$. With any finitely generated right-module M of the ring $K_R A_L$, which possesses the unit element of $K_R A_L$ as an identity operator, we have*

$$M = M_0 \times_{C_L} A_L ,$$

where M_0 is the totality of elements w in M such that $w\,k_R = w\,k_L$ for every $k \in K$.

PROOF. Immediate from Theorem 1 and the accompanying Remark, for $w\,k_R = w\,k_L$ gives $w\,a_L\,k_R = w\,k_R\,a_L = w\,k_L\,a_L = w\,(a\,k)_L$ for every $a \in A$ (and conversely, since $1 \in A$).

THEOREM 3. *Let A, K be as in Theorem 2. If S is a ring which contains A as its subring, whose center contains the center Z of A and which possesses the unit element of A as its unit element, then*

$$S = A \times_C V_S(K) .$$

PROOF. We consider S as a $K_R A_L$-right-module on defining[10)]

$$v\,k_R = v\,k\,, \qquad v\,a_L = a\,v \qquad (v \in S,\ \ k \in K,\ \ a \in A).$$

The module M_0, in Theorem 2, with $M = S$ is the totality of elements w in S such that $w\,k_R = w\,k_L$, or $w\,k = k\,w$, for every $k \in K$. Thus $M_0 = V_S(K)$, and $S = V_S(K) \times_C A_L$.

10) This is allowed, as $K_R \frown L_L = Z_R\ (= Z_L)$ and Z is contained in the center of S.

PROPOSITION 7. *Let A, K and S be as in Theorem 3. Then S is innerly weakly normal over its subring $V_S(K)$.*

PROOF. K possesses an independent basis $(k_1, k_2, \cdots, k_n)$ over the center Z of A. There exists a system of n elements $a_1, a_2, \cdots, a_n$ in A, forming in fact an independent right-basis of A over C, such that the matrix $(a_j k_i)_{ij}$ in A is regular. It is regular also as an matrix in S. Hence, by Proposition 5, S is innerly weakly normal over its subring $V_S(K)$.

PROPOSITION 8. *Let A be innerly weakly normal over its subring C. If C is simple, both A and K are simple. If C satisfies the right (or left) minimum condition and is primary, both A and K are primary.*

PROOF. We have $V_{\mathfrak{A}}(C_R)=K_R \times_{Z_R} A_L=\sum k_{iR} A_L$, where Z is the center of A and $k_{1R}, k_{2R}, \cdots, k_{nR}$ are independent over A_L. If $\mathfrak{a}$ is a proper ideal of A, $K_R \mathfrak{a}_L$ is a proper ideal of $V_{\mathfrak{A}}(C_R)$. Now, if C is simple, then $V_{\mathfrak{A}}(C_R)$, a matric ring (of finite degree n) over a ring inversely isomorphic to C, is simple too. It follows that A is simple too. Its center Z is a field then, and A possesses an independent (possibly infinite) basis over Z. We see, similarly as above, that K is simple too. Suppose next that C satisfies the right (left) minimum condition and is primary. Then $V_{\mathfrak{A}}(C_R)$ (satisfies the left (right) minimum condition and) is primary. Let N be the radical of A. If A/N were (two-sided) directly decomposable, then $V_{\mathfrak{A}}(C_R)/K_R N_L=K_R A_L/K_R N_L$ would be directly decomposable. So A must be primary. Further, K is semi-primary, as the endomorphism ring of a module with composition-series. A proper direct decomposition of its residue-ring K/Q module its radical Q would entail a such of $V_{\mathfrak{A}}(C_R)/Q_R A_L=K_R A_L/Q_R A_L$; consider orthogonal central idempotent elements in K/Q. Thus K must be primary too.

PROPOSITION 9. *Let A satisfy the minimum condition and be primary and innerly weakly normal over its subring C. Let B be a subring of A which contains C and over which A possesses an independent right-basis. Then A is innerly weakly normal over B.*

This was proved in [5], Theorem (3. 2).

THEOREM 4. *Let A, and B be as in Proposition 9, and assume that B is primary (together with A). If α is an isomorphism of B into A leaving C elementwise fiexd, and if A has an independent* *right-basis over B^α too, then α can be extended to an inner automorphism of A. In particular, every automorphism of A leaving C elementwise fixed is inner.*

This is a generalization of [7], Theorem 1. We shall not prove the theorem here, since we shall give, and prove, a further generalization in a paper sequel to [6].

§ 4. Inner weak normality over (a subring contained in) the center.

We now consider the case where the subring C (containing the unit element 1 of A) is contained in the center Z of A. We again assume that A has an independent finite basis over C. On generalizing the notion of maximally central algebras introduced in the joint paper Azumaya-Nakayama [2], the former author called, in [1], A to be proper maximally central over C when the $C_R(=C_L)$-endomorphism ring $V_{\mathfrak{A}}(C_R)$ of A is the Kronecker product $A_R \times A_L$ over C_R. This is nothing but the present case $C \leq Z$ of our inner weak normality. For, the proper maximal centrality of A over C evidently implies that A is innerly weakly normal over C. The converse follows from our Proposition 5 and Azumaya's [1] Theorem 12.

We observe that $K=V_A(C)=A$ for $C \leq Z$, and we see, when A is innerly weakly normal (i. e. proper maximally central) over C, that $C=V_A(K)=V_A(A)=Z$, that is, C coincides with the center Z. Further, submodules of A allowable with respect to $V_{\mathfrak{A}}(C)=A_R A_L$ are nothing but two-sided ideals of A. Thus our Proposition 6 is a generalization of Azumaya's [1] Theorem 13. Our Theorem 2 generalizes his Theorem 16, whence it (or its corollary Theorem 3) forms a generalization of a well-known theorem of Wedderburn alluded to in the introduction (that if, a central simple finite-dimensional algebra A, over a field C, is contained, as a subalgebra, in an algebra S, over C, and contains the unit element of S, then S is the Kronecker product $V_S(A) \times A$. On the other hand, our Theorem 4 is of a nature rather different from Theorem 18 of Azumaya [1] (though it has also as a corollary the Corollary to Azumaya [1], Theorem 18).

§ 5. Semigroup of weakly normal rings over a commutative ring.

In this section we again consider the case where the underlying subring is (commutative and) contained in the center.

PROPOSITION 10. *If two rings A, B are weakly normal over their common subring C contained in their centers, then the Kronecker product ring $A\times_C B$ over C is weakly normal over C. If A, B are innerly weakly normal over C, then $A\times_C B$ is innerly weakly normal over C too.*

PROOF. We have $V_{\mathfrak{A}}(C_R)=\gamma_1 A_L \oplus \gamma_2 A_L \oplus\cdots\oplus \gamma_n A_L$ with A_L-semilinear endomorphisms $\gamma_1, \gamma_2, \cdots \gamma_n$ of A. Similary

$$V_{\mathfrak{B}}(C_{R(B)})=\delta_1 B_{L(B)} \oplus \delta_2 B_{L(B)} \oplus\cdots\oplus \delta_m B_{L(B)}$$

with $B_{L(B)}$-semilinear endomorphisms $\delta_1, \delta_2, \cdots, \delta_m$ of B, where $\mathfrak{B}$ is the absolute endomorphism ring of B and $C_{R(B)}$, $B_{L(B)}$ denote the right (or left) and left multiplication rings of C and B, respectively, onto B. Identifying C with C_R and $C_{R(B)}$, we may consider C as a common subring of $\mathfrak{A}$ and $\mathfrak{B}$. Then the C-endomorphism ring of $A\times_C B$ is the Kronecker product of $V_{\mathfrak{A}}(C_R)$ and $V_{\mathfrak{B}}(C_{R(B)})$ over C, and is thus

$$\sum \gamma_i \delta_j (A_L\times_C B_{L(B)}) .$$

Here $\gamma_i \delta_j$ are $A_L\times_C B_{L(B)}$-semilinear endomorphisms of $A\times_C B$. Furthermore, $A_L\times_C B_{L(B)}$ may be identified with the left-multiplication ring of $A\times_C B$. Thus $A\times_C B$ is weakly normal over C. If moreover A, B are innerly weakly normal over C, then γ_i and δ_j may be chosen to be A_L- and $B_{L(B)}$-linear, respectively. Then $\gamma_i \delta_j$ are $A_L\times_C B_{L(B)}$-linear and $A\times_C B$ is innerly weakly normal over C.

COROLLARY. *Let A be (innerly) weakly normal over a subring C contained in the center. Then a matric ring $(A)_k$ of a finite degree k is (innerly) weakly normal over C (C being considered as a subring of $(A)_k$).*[11]

11) As a matter of fact, the converse is true too, provided that we assume that A possesses an independent basis over C; see Theorem 5 below. Moreover, this last preassumption is unnecessary if C satisfies the minimum condition (or if the residue-ring of C modulo its radical satisfies the minimum condition; cf. Corollary to Theorem 3 in Azumaya [1]).

For, the matric ring $(C)_k$ is innerly weakly normal over C, as one readily sees by means of Proposition 5, for instance.

Clearly the Kronecker product over C of the matric rings $(C)_k$ and $(C)_l$ is the matric ring $(C)_{kl}$. Azumaya [1] classified rings innerly weakly normal over C and possessing C as their center (i. e. proper maximally central over C) by means of the semigroup of matric rings over C, to the effect to have a generalization of the celebrated Brauer group of algebra-classes (of central simple algebras over a field). We are led, by the above observations, to consider, more generally, the following semigroups of rings.

Let, namely, C be a commutative ring, with unit element. We denote by $\mathfrak{R}_1(C)$ the semigroup of all rings containing C in their center, possessing the unit element of C as their unit element and possessing independent finite bases over C; the multiplication being the Kronecker product multiplication over C, and rings isomorphic over C being considered as identical. Let $\mathfrak{R}_2(C)$ and $\mathfrak{R}_3(C)$ be the subsemigroups of $\mathfrak{R}_1(C)$ consisting of those rings which are weakly normal and innerly weakly normal over C, respectively. Let, further, $\mathfrak{R}_4(C)$ be the semigroup of matric rings, of finite degrees, over C; $\mathfrak{R}_1(C) \supseteq \mathfrak{R}_2(C) \supseteq \mathfrak{R}_3(C) \supseteq \mathfrak{R}_4(C)$.

Then the factor-semigroup[12] $\mathfrak{R}_3(C)/\mathfrak{R}_4(C)$ is actually a group (cf. Azumaya [1]). For, if $A \in \mathfrak{R}_3(C)$ then $A_R \times_C A_L$ is $V_{\mathfrak{A}}(C_R)$ and is a matric ring (of finite degree) over C. Here A_R is isomorphic, over C, to A (and A_L is inversely isomorphic to A). Now we have

THEOREM 5. *Let C be a commutative ring with unit element whose residue-ring module the radical satisfies the minimum condition. Then, $\mathfrak{R}_3(C)/\mathfrak{R}_4(C)$ is the largest subgroup of the semigroup $\mathfrak{R}_1(C)/\mathfrak{R}_4(C)$. In fact, in the semigroup $\mathfrak{R}_1(C)/\mathfrak{R}_3(C)$ the unit element $\mathfrak{R}_3(C)/\mathfrak{R}_3(C)$ is the largest subgroup. More precisely, if $A, B \in \mathfrak{R}_1(C)$ and $A \times_C B \in \mathfrak{R}_3(C)$, then necessarily $A, B \in \mathfrak{R}_3(C)$.*

PROOF. Let $A, B \in \mathfrak{R}_1(C)$, and let

$$V_{\mathfrak{A}}(C_R) = \gamma_1 A_L \oplus \gamma_2 A_L \oplus \cdots \oplus \gamma_n A_L,$$

$$V_{\mathfrak{B}}(C_{R(B)}) = \delta_1 B_{L(B)} \oplus \delta_2 B_{L(B)} \oplus \cdots \oplus \delta_m B_{L(B)},$$

12) Two elements A, B in $\mathfrak{R}_3(C)$ are set to be equivalent when there are A_1, B_1 in $\mathfrak{R}_4(C)$ such that $A \times A_1 = B \times B_1$.

where γ_i and δ_j are some elements of the absolute endomorphism rings $\mathfrak{A}$ and $\mathfrak{B}$ of A and B, respectively, and $C_{R(B)}(=C_{L(B)})$, $B_{L(B)}$ are the right and left multiplication rings of C, B onto B, Then the C-endomorphism ring of $A\times_C B$ is $V_{\mathfrak{A}}(C_R)\times_C V_{\mathfrak{B}}(C_{R(B)})$, as before. Considered as an $A_L\,(\subseteq V_{\mathfrak{A}}(C_R))$-two-sided module, it is thus isomorphic to the direct sum of m^2 isomorphic copies of $V_{\mathfrak{A}}(C_R)$. Now, suppose that $A\times_C B$ is innerly weakly normal over C, i. e. $A\times_C B\in\mathfrak{R}_3(C)$. Then the C-endomorphism ring of $A\times_C B$ is a direct sum of submodules of form $\omega_k(A\times_C B)_{L(A\times B)}$, with ω_k elementwise commutative with $(A\times_C B)_{L(A\times B)}=A_L\times_C B_{L(B)}$, the left multiplication ring of $A\times_C B$. Thus it is, considered as an A_L-two-sided module, isomorphic to a direct sum of isomorphic copies of A_L. It follows[13] that the A_L-two-sided module $V_{\mathfrak{A}}(C_R)$ is isomorphic to a direct sum of isomorphic copies of A_L. This means however that A is innerly weakly normal over C. Similarly $B\in\mathfrak{R}_3(C)$. Our theorem is thus proved.

Let, next D be a commutative ring which contains C as its subring and possesses the unit element of C as its unit element. As the usual coefficient field extension for algebras, we may form from each ring A in $\mathfrak{R}_1(C)$ a ring $A\times_C D\in\mathfrak{R}_1(D)$. In this way we obtain a natural homomorphic mapping of $\mathfrak{R}_1(C)$ into $\mathfrak{R}_1(D)$, and it is clear that $\mathfrak{R}_2(C)$, $\mathfrak{R}_3(C)$ and $\mathfrak{R}_4(C)$ are mapped into $\mathfrak{R}_2(D)$, $\mathfrak{R}_3(D)$ and $\mathfrak{R}_4(D)$, respectively, by this homomorphism. Now, provided that C satisfies the same condition as in Theorem 5 and that D possesses an independent finite[14] basis over C, *the mapping of* $\mathfrak{R}_1(C)/\mathfrak{R}_3(C)$ *into* $\mathfrak{R}_1(D)/\mathfrak{R}_3(D)$ *is an (into-) isomorphic mapping.* This we can see in similar manner as above, considering that the D-endomorphism ring of $A\times_C D$ is the ring $V_{\mathfrak{A}}(C_R)\times_C D_{R(D)}$, where $D_{R(D)}$ is the right multiplication ring of D (onto D).

Note that $A\times_C D$ can belong to $\mathfrak{R}_2(D)$ even when $A\notin\mathfrak{R}_2(C)$; let for example A be a non-normal (but separable) finite extension of a field C and D be the splitting Galois field of A over C;[15] or, we may take as C, A, D respectively the rational number field, $C(\sqrt[3]{2})$, and

13) Azumaya [1], Corollary to Theorem 4.

14) If C satisfies the minimum condition, the finiteness assumption is unnecessary.

15) If $A\times_C D=e_1D\oplus e_2D\oplus\cdots\oplus e_nD$ with mutually orthogonal (primitive) independent elements e_i, then the cyclic permutations of $(e_1, e_2,\cdots, e_n)$ over D generate over $(A\times_C D)_{L(A\times D)}$ the endomorphism ring of $A\times_C D$.

$C(\omega)$, ω being a primitive 3rd root of unity.[16] The same examples serve to show,[17] in connection of Theorem 5, that $A \times_C B$ can belong to $\mathfrak{R}_2(C)$ even when at least one of A, B does not belong to $\mathfrak{R}_2(C)$; let $B=D$. Moreover, $A \times_C B$ may belong to $\mathfrak{R}_2(C)$ even when both A, and B fail to belong to $\mathfrak{R}_2(C)$. Consider for example a Galois extension over a field C whose Galois group is a product of two mutually disjoint, mutually permutable, non-normal subgroups, and let A, B be the fields belonging to these subgroups.

Appendix. Inverse of Wedderburn's theorem.

The following inverse of Wedderburn's theorem has been communicated to the writer by N. Jacobson:

Let A be a (finite- or infinite-dimensional) algebra with unit element 1 *over a field C, and suppose that every algebra S over C containing A, as a subalgebra, and having as its unit element the unit element* 1 *of A is decomposed into a Kronecker product, over C, of A and a second subalgebra. Then A is simple, central and finite-dimensional (i. e. innerly weakly normal) over C.*

We shall give here a simple proof to this theorem. Let, to do so, $\mathfrak{A}_0$ be the ring of all C-endomorphisms of A. The right and left multiplication rings A_R and A_L of A are subrings of $\mathfrak{A}_0$ and they are the commuters of each other. As A_R is isomorphic to A (over C), $\mathfrak{A}_0$ must be decomposable into a Kronecker product, over C, of A_R and a second subalgebra, say $\mathfrak{B}$: $\mathfrak{A}_0 = A_R \times_C \mathfrak{B}$. Here $\mathfrak{B} \leq V_{\mathfrak{A}_0}(A_R) = A_L$. So $(\mathfrak{A}_0 : C) = (A_R : C)(\mathfrak{B} : C) \leq (A_R : C)(A_L : C) = (A : C)^2$. We assert that the rank $(A : C)$ is finite. For, if $(A : C)$ were infinite, then the (infinite) rank $(\mathfrak{A}_0 : C)$ (of the full column-finite matric ring $\mathfrak{A}_0$) of dimension $(A : C)$ over C) would be greater than $(A : C)^2 = (A : C)$ (in virtue of the fact that $2^{\mathfrak{a}} > \mathfrak{a}$ for every cardinal $\mathfrak{a}$). Thus $(A : C)$ is finite, and (the full matric ring of dimension $(A : C)$ over C) $\mathfrak{A}_0$ is a

16) Observe that the field $C(\omega, \sqrt[3]{2})$ is the Kronecker product of $C(\omega)$, $C(\sqrt[3]{2})$ over C and is normal over C (while $C(\sqrt[3]{2})$ is not normal over C).

17) In the first example, consider the automorphism group of $A \times_C D$ over C generated by the cyclic permutations of $(e_1, e_2, \cdots, e_n)$ and the Galois group of D/C. In constructing these examples I owe a kind remark to G. Hochschild.

central simple algebra, over C. Hence its Kronecker factor A_R is a central simple algebra too. As A_R is isomorphic to A, this proves our theorem.

References

[1] G. Azumaya, On maximally central algebras, Nagoya Math. J., 2 (1951), 119-150.

[2] G. Azumaya-T. Nakayama, On absolutely uni-serial algebras, Jap. J. Math., 19 (1948), 263-273.

[3] J. Dieudonné, La théorie de Galois des anneaux simples et semi-simples, Comment. Math. Helv., 21 (1948), 154-184.

[4] N. Jacobson, The radical and semi-simplicity for arbitray rings, Amer. J. Math., 67 (1945), 300-320.

[5] T. Nakayama, Commuter systems in a ring with radical, Duke Math. J., 16 (1949) 331-337.

[6] ———, Generalized Galois theory for rings with minimum condition, Amer. J. Math., 73 (1951), 1-12.

[7] ———, Automorphisms of simple, complete primitive, and directly indecomposable rings, Ann. Math., 55 (1952) 538-551.

[8] ———, Note on double-modules over arbitrary rings, Amer. J. Math., 74 (1952), 645-655.

[9] ———, Derivation and cohomology in simple and other rings,I, Duke Math. J., 19 (1952), 51-63.

[10] ———, Galois theory of simple rings, Trans. Amer. Math. Soc. 73 (1952), 276-292.