Journal of the Mathematical Society of Japan Vol. 1, No. 2, July, 1949.

Galois theory for uni-serial rings.

Gôrô AZUMAYA.

(Received Dec. 29, 1947)

In a previous paper[1], I have given a new method to the theory of simple rings, which enables us in particular to prove the fundamental theorem of simple rings in a quite natural way as well as to extend the Jacobson's Galois theory[2] from quasi-fields to simple rings; our principal method was in fact to embed the simple ring into an absolute endomorphism ring (of a certain module) and take commuter ring in it. In this paper we shall show that by means of the similar method these results can be extended completely to the uni-serial case[3] and shall obtain some other detailed results which have significance even in the case of simple rings. Further, after establishing the Galois theory, we shall give a new and simpler proof to the existence theorem of normal bases[4].

Throughout the present paper, we mean by a ring always one possessing an unit element and by a subring always one whose unit element coincides with that of the original ring, and when we deal with a module with operator-ring we assume always that the unit element of the latter operates on the former as the identity endomorphism. Further, when $\mathfrak{S}$ is a subring of a ring $\mathfrak{R}$, we denote by $V_{\mathfrak{R}}(\mathfrak{S})$ the commuter ring of $\mathfrak{S}$ in $\mathfrak{R}$.

For the sake of completeness, let us begin with the following consideration concerning moduli with operator-ring:

§ 1. Moduli with operator-ring and their submoduli.

Lemma 1.[5] *Let $\mathfrak{R}$ be a two-sided simple ring*[6] *with the center Z*[7] *and*

1) Azumaya [2]. Cf. also Nakayama-Azumaya [13].

2) Jacobson [6].

3) While their extention to irreducible rings is treated in Nakayama-Azumaya [13].

4) In case of quasi-fields, this theorem was proved in Nakayama [12]. The same method can readily be transferred to the case of simple rings. However, it can no longer, as it seems to the writer, apply to our case.

5) Cf. Kurosh [8].

6) By a two-sided simple ring we understand a ring which possesses no non-trivial two-sided ideal, while if a two-sided simple ring satisfies the minimum condition for right (or equivalently left) ideals we call it a simple ring.

7) Z forms a (commutative) field.

let there be given an $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module $\mathfrak{M}$ such that $\mathfrak{M}=\mathfrak{N}\mathfrak{R}$, where $\mathfrak{N}$ is the Z-module consisting of all elements of $\mathfrak{M}$ which are element-wise commutative with $\mathfrak{R}$. Then

1) *$\mathfrak{M}$ is the direct product of $\mathfrak{N}$ and $\mathfrak{R}$ (over Z): $\mathfrak{M}=\mathfrak{N}\times\mathfrak{R}$.*

2) *Between $\mathfrak{R}$-$\mathfrak{R}$-submoduli $\mathfrak{M}_0$ of $\mathfrak{M}$ and Z-submoduli $\mathfrak{N}_0$ of $\mathfrak{N}$, there is a one-to-one correspondence by the following relation:*

$$\mathfrak{M}_0=\mathfrak{N}_0\mathfrak{R},\quad \mathfrak{N}_0=\mathfrak{M}_0\frown\mathfrak{N}.$$

3) *An element $u\in\mathfrak{M}$ satisfies $\mathfrak{R}u=u\mathfrak{R}$ if and only if there exists a regular element c in $\mathfrak{R}$ such that $xu=u(c^{-1}xc)$ for every $x\in\mathfrak{R}$.*

Proof. First it is to be observed that an ($\mathfrak{R}$-$\mathfrak{R}$-) submodule $\mathfrak{m}$ of $\mathfrak{M}$ is (non-zero and operator-homomorphic whence) operator-isomorphic to the simple module $\mathfrak{R}$ if and only if there exists an element $v\neq 0$ in $\mathfrak{N}$ such that $\mathfrak{m}=v\mathfrak{R}$; and, when this is the case, the isomorphism is given by $x\rightarrow(xv=)vx$ $(x\in\mathfrak{R})$. Now since $\mathfrak{M}=\mathfrak{N}\mathfrak{R}=\bigcup_{v\in\mathfrak{N}} v\mathfrak{R}$[8] is completely reducible, $\mathfrak{M}$ is indeed expressed as the direct sum of a number of simple submoduli $v\mathfrak{R}$; that is, we can find a subset $\{v_\mu\}$ of $\mathfrak{N}$ linearly independent over $\mathfrak{R}$ such that $\mathfrak{M}=\sum_\mu v_\mu\mathfrak{R}$. Then we have readily $\mathfrak{N}=\sum_\mu v_\mu Z$, which shows the the assertion 1). Further, since every submodule $\mathfrak{M}_0$ of $\mathfrak{M}$ is also completely reducible, $\mathfrak{M}_0$ is the (finite or infinite direct) sum of simple submoduli of the form $v\mathfrak{R}(v\in\mathfrak{N})$, i.e. $\mathfrak{M}_0=\mathfrak{N}_0\mathfrak{R}$ provided $\mathfrak{N}_0=\mathfrak{M}_0\frown\mathfrak{N}$. Conversely, since the product $\mathfrak{N}_0\mathfrak{R}=\mathfrak{N}_0\times\mathfrak{R}$ is direct for any (Z-) submodule $\mathfrak{N}_0$ of $\mathfrak{N}$, it follows $\mathfrak{N}_0=\mathfrak{M}_0\frown\mathfrak{N}$ when $\mathfrak{M}_0=\mathfrak{N}_0\mathfrak{R}$. Thus 2) is proved. To prove 3), let $u\neq 0$ satisfy $\mathfrak{R}u=u\mathfrak{R}$. Then this is simple, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, and hence operator-isomorphic with $\mathfrak{R}$ i.e. there exists an element v in $\mathfrak{N}$ such that $u\mathfrak{R}=v\mathfrak{R}$; this means also the existence of a regular element c in $\mathfrak{R}$ such that $u=vc$ whence $xu=xvc=uxc=uc^{-1}xc$ for every $x\in\mathfrak{R}$. The converse is evident.

From this lemma we have immediately

Theorem 1. *Let $\mathfrak{P}$ be a ring and $\mathfrak{R}$ be a two-sided simple subring of $\mathfrak{P}$ whose center Z is contained in the center of $\mathfrak{P}$ and let $\mathfrak{S}$ be the commuter ring of $\mathfrak{R}$ in $\mathfrak{P}$: $\mathfrak{S}=V_{\mathfrak{P}}(\mathfrak{R})$. If $\mathfrak{P}=\mathfrak{R}\mathfrak{S}$,* then

1) *$\mathfrak{P}$ is the direct of $\mathfrak{R}$ and $\mathfrak{S}$ (over Z): $\mathfrak{P}=\mathfrak{R}\times\mathfrak{S}$.*

2)[9] *Between two-sided ideals $\mathfrak{p}$ of $\mathfrak{P}$ and two-sided ideals $\mathfrak{s}$ of $\mathfrak{S}$, be-*

---

8) $\bigcup$ means module sum.

9) Cf. Noether [14], Kurosh [8].

tween left [right] ideals $\mathfrak{p}$ *of* $\mathfrak{P}$ *which are right-[left-]allowable with respect to* $\mathfrak{S}$ *and left [right] ideals* $\mathfrak{s}$ *of* $\mathfrak{S}$, *or between subrings* $\mathfrak{p}$ *of* $\mathfrak{P}$ *which contain* $\mathfrak{R}$ *and subrings* $\mathfrak{s}$ *of* $\mathfrak{S}$ *which contain* Z, *there exists a one-to-one correspondence by the following relation:*

$$\mathfrak{p}=\mathfrak{s}\times\mathfrak{R}, \quad \mathfrak{s}=\mathfrak{p}\frown\mathfrak{S}.$$

3) *An automorphism of* $\mathfrak{R}$ *can be extended to an inner automorphism of* $\mathfrak{P}$ *if and only if it is already inner in* $\mathfrak{R}$.

Now we may refine readily Nakayama-Azumaya [13], Lemma 1 as follows:

Lemma 2. *Let* $\mathfrak{M}$ *be a right module of a ring* $\mathfrak{R}$ *and let* $\mathfrak{M}=\sum_\mu \mathfrak{m}_\mu$ *be a direct decomposition of* $\mathfrak{M}$ *into mutually operator-isomorphic* $\mathfrak{R}$*-submoduli* $\mathfrak{m}_\mu$. *Take an arbitrary direct summnd* $\mathfrak{m}_0$ *and let* $\mathfrak{R}^*$ *and* $\mathfrak{R}_0$ *be the operator-endomorphism ring of* $\mathfrak{M}$ *and* $\mathfrak{m}_0$ *respectively. Then*

1) *There exists a one-to-one correspoudence between* $\mathfrak{R}^*$*-submoduli* $\mathfrak{N}$ *of* $\mathfrak{M}$ *and* $\mathfrak{R}_0$*-submoduli* $\mathfrak{n}_0$ *of* $\mathfrak{m}_0$ *by the following relation,*

$$\mathfrak{N}=\sum_\mu \mathfrak{n}_\mu$$

where $\mathfrak{n}_\mu$ *is, for each* μ, *the submodule of* $\mathfrak{m}_\mu$ *correiponding to* $\mathfrak{n}_0$. *Further, for any element* a *in* $\mathfrak{R}$, $\mathfrak{N}$ *is allowable with respect to* a *if and only if* $\mathfrak{n}_0$ *may be.*

2) $\mathfrak{R}$ *may be considered as the* $\mathfrak{R}^*$*-endomorphism ring of* $\mathfrak{M}$ *if aud only if* $\mathfrak{R}$ *is considered as the* $\mathfrak{R}_0$*-endomorphism ring of* $\mathfrak{m}_0$. *The "if" part also holds even in case when every* $\mathfrak{m}_\mu$ *is (not necessarily operator-isomorphic but) operator-homomorphic to* $\mathfrak{m}_0$.

Now, let us say that a right module $\mathfrak{M}$ of a ring $\mathfrak{R}$ is (*right-*) *regular* (with respect to $\mathfrak{R}$) if there exists a (direct summand) right ideal $\mathfrak{r}_0$ of $\mathfrak{R}$ such that both $\mathfrak{M}$ and $\mathfrak{R}$ directly decomposable into submoduli each of which is operator-isomorphic to $\mathfrak{r}_0$.

Theorem 2. *Let* $\mathfrak{M}$ *be a regular right module of* $\mathfrak{R}$ *and let* $\mathfrak{R}^*$ *be its operator-endomorphism ring. Then*

1) *There exists a one-to-one correspondence between* $\mathfrak{R}^*$*-submoduli and left ideals* $\mathfrak{l}$ *of* $\mathfrak{R}$ *by the following relation:*

$$\mathfrak{N}=\mathfrak{M}\mathfrak{l}.^{10)}$$

---

10) Conversely, $\mathfrak{l}$ is characterized by $\mathfrak{N}$ as the set of all elements a in $\mathfrak{R}$ such that $\mathfrak{M}a\subseteq\mathfrak{N}$.

Further, when $\mathfrak{N}\longleftrightarrow\mathfrak{l}$, $\mathfrak{N}$ *is allowable with respect to an element* a *in* $\mathfrak{R}$ *if and only if* $\mathfrak{l}$ *is so.*

2) $\mathfrak{R}$ *may be considered as the* $\mathfrak{R}^*$*-endomorphism ring of* $\mathfrak{M}$; *the same is the case also when* $\mathfrak{M}$ *is a direct sum of submoduli each of which is operator-homomorphic to* $\mathfrak{r}_0$ *and at least one of them is operator-isomorphic to* $\mathfrak{r}_0$.

3) *If* $\mathfrak{M}$ *is finite with respect to* $\mathfrak{R}$, *then* $\mathfrak{M}$ *is also regular and finite with respect to* $\mathfrak{R}^*$.

Proof. $\mathfrak{r}_0$ is generated by an idempotent element e; $\mathfrak{r}_0=e\mathfrak{R}=e\mathfrak{r}_0$, and (the left operator-ring) $e\mathfrak{R}e$ can be, as usual, regarded as the operator-endomorphism ring or $\mathfrak{r}_0$. Suppose $\mathfrak{M}=\sum_\mu \mathfrak{m}_\mu$ be a direct decomposition of $\mathfrak{M}$ into submoduli $\mathfrak{m}_\mu$ operator-isomorphic to $\mathfrak{r}_0$ and consider any $e\mathfrak{R}e$-submodule $\mathfrak{s}_0$ of $\mathfrak{r}_0$. Then, since $\mathfrak{s}_0=e\mathfrak{R}e\mathfrak{s}_0=\mathfrak{r}_0\mathfrak{s}_0$, the submodule of $\mathfrak{m}_\mu$ corresponding to $\mathfrak{s}_0$ is $\mathfrak{m}_\mu\mathfrak{s}_0$. In virtue of the preceding lemma, every $\mathfrak{R}$-submodule $\mathfrak{N}$ is uniquely expressed as $\mathfrak{N}=\sum_\mu \mathfrak{m}_\mu\mathfrak{s}_0=\mathfrak{M}\mathfrak{s}_0$ by an $e\mathfrak{R}e$-submodule $\mathfrak{s}_0$ of $\mathfrak{r}_0$. Similarly, every left ideal $\mathfrak{l}$ of $\mathfrak{R}$ can be uniquely expressed in the form $\mathfrak{l}=\mathfrak{R}\mathfrak{s}_0$ by $\mathfrak{s}_0$. Combining these, we have $\mathfrak{N}=\mathfrak{M}\mathfrak{s}_0=\mathfrak{M}\mathfrak{R}\mathfrak{s}_0=\mathfrak{M}\mathfrak{l}$.

Now, since $\mathfrak{R}$ is a direct sum of a finite number, say r, of right ideals operator-isomorphic with $\mathfrak{r}_0$, we can construct as usual a system of matrix units $\{e_{ij};\ i, j=1, 2, \ldots\ldots, r\}$ in $\mathfrak{R}$ linearly independent with respect to its commuter ring $\mathfrak{R}_0$ in $\mathfrak{R}$ such that $\mathfrak{R}=\sum_{i,j}\mathfrak{R}_0 e_{ij}$ and $\mathfrak{r}_0=\sum_j \mathfrak{R}_0 e_{1j}$; $\mathfrak{R}_0$ is considered naturally as the operator-endomorphism ring of (the right ideal) $\mathfrak{r}_0$ and conversely $\mathfrak{R}$ can be looked upon as the $\mathfrak{R}_0$-endomorphism ring of the r-dimensional vector module $\mathfrak{r}_0$ (over $\mathfrak{R}_0$). From this follows directly the assertion 2), by virtue of Lemma 2, 2). To prove 3), we may assume that $\mathfrak{R}$ is in fact the r-dimensional matrix ring over $\mathfrak{R}_0$ and $\mathfrak{r}_0$ is the r-dimensional row-vector space over $\mathfrak{R}_0$ and further $\mathfrak{M}$ is finite, say n-, dimensional column-vector space over $\mathfrak{r}_0$, that is, the totality of matrices of type (n, r) over $\mathfrak{R}_0$. $\mathfrak{R}^*$ is therefore nothing but the n-dimensional matrix ring over $\mathfrak{R}_0$, considered as left operator-ring of $\mathfrak{M}$. Then the fact that $\mathfrak{R}^*$ and $\mathfrak{M}$ are respectively the n-dimensional and r-dimensional row-vector spaces over the n-dimensional column-vector space over $\mathfrak{R}_0$ implies that $\mathfrak{M}$ is finite and regular with respect to $\mathfrak{R}^*$.

Corollary. *Let* $\mathfrak{M}$ *be finite and regular with respect to* $\mathfrak{R}$ *and let* $\mathfrak{R}^*$ *be its operator-endomorphism ring. Then between* $\mathfrak{R}$-$\mathfrak{R}^*$*-submoduli* $\mathfrak{N}$, *two-sided ideals* $\mathfrak{a}$ *of* $\mathfrak{R}$ *and two-sided ideals* $\mathfrak{a}^*$ *of* $\mathfrak{R}^*$ *there exists a one-to-one* *correspondence by the following relation:* $\mathfrak{N}=\mathfrak{M}\mathfrak{a}=\mathfrak{M}\mathfrak{a}^*$.

Finally we point out the following simple fact:

Lemma 3. *Let* $\mathfrak{M}$ *be an* $\mathfrak{R}$*-right-module which is operator-isomorphic with* $\mathfrak{R}$ *and let* $\mathfrak{R}^*$ *be its operator-endomorphism ring. Then* $\mathfrak{M}$ *is, as* $\mathfrak{R}^*$*-module, operator-isomorphic with* $\mathfrak{R}^*$*; further for any element* u *of* $\mathfrak{M}$ *such that the mapping* $1 \to u$ *gives an operator-isomorphism between* $\mathfrak{R}$ *and* $\mathfrak{M}$ *the mapping* $1^* \to u$ *also gives an* $\mathfrak{R}^*$*-isomorphism between* $\mathfrak{R}^*$ *and* $\mathfrak{M}$*, where* 1 *and* 1^* *denote the unit element of* $\mathfrak{R}$ *and* $\mathfrak{R}^*$ *respectively.*

§ 2. Moduli with uni-serial operator-ring.

Let $\mathfrak{R}$ be a ring satisfying the minimum (whence the maximum) condition for left and right ideals and let $\mathfrak{C}$ be its radical. $\mathfrak{R}$ is called *primary* if the residue class ring $\bar{\mathfrak{R}}=\mathfrak{R}/\mathfrak{C}$ is simple. For that it is necessary and sufficient that $\mathfrak{R}$ is decomposable into a direct sum of mutually operator-isomorphic directly indecomposable right (or left) ideals. And, when this is the case, the number of right (or left) ideals is independent of the direct decomposition; we shall denote the number by $[\mathfrak{R}]$.

A primary ring $\mathfrak{R}$ is called *uni-serial*[11] if every (or equivalently at least one) directly indecomposable direct summand right or left ideal, that is, the right ideal $e\mathfrak{R}$ as well as the left ideal $\mathfrak{R}e$ generated by a primitive idempotent element e possesses only one composition series. For that it is necessary and sufficient that $\mathfrak{C}$ is a principal two-sided ideal (generated by a single element c); $\mathfrak{C}=\mathfrak{R}c=c\mathfrak{R}$. And, when this is the case, the right ideals $e\mathfrak{R}$, $e\mathfrak{C}$, $e\mathfrak{C}^2$, ..., $e\mathfrak{C}^{l-1}$, $e\mathfrak{C}^l=0$ form in fact the only composition series of $e\mathfrak{R}$, where l is the exponent of the radical $\mathfrak{C}$; the similar is also true for $\mathfrak{R}e$.

Now let $\mathfrak{M}$ be a right module of a primary uni-serial ring $\mathfrak{R}$. Then $\mathfrak{M}$ is, in virtue of the main theorem of uni-serial rings, directly decomposed into (directly indecomposable and cyclic) submoduli operator-homomorphic to $e\mathfrak{R}$, and the direct decomposition is, by Krull-Remak-Schmidt theorem[12] for instance, unique up to operator-isomorphism. It is obvious that $\mathfrak{M}$ *is regular with respect to* $\mathfrak{R}$ *if and only if* every directly indecomposable direct

11) For uni-serial (=einreihig) rings, see Köthe [7], Asano [1], Nakayama [11], Azumaya-Nakayama [5].

12) See Azumaya [4].

summand is operator-isomorphic to $e\mathfrak{R}$, or what is the same, *every (not necessarily directly indecomposable) direct summand is faithful with respect to* $\mathfrak{R}$[13]. We denote, when this is the case, by $[\mathfrak{M}\mid\mathfrak{R}]$ the (cardinal) number of direct summands (appearing in a direct decomposition) of $\mathfrak{M}$. $\mathfrak{M}$ possesses linearly independent *(right-)basis* over $\mathfrak{R}$ if and only if $\mathfrak{M}$ is regular and moreover $[\mathfrak{M}\mid\mathfrak{R}]$ is divisible by $[\mathfrak{R}]$[14]. And, when this is the case, the number of elements consitituting 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 $[\mathfrak{M}:\mathfrak{R}]$.

Observing that if we embed $\mathfrak{R}$ into the absolute endomorphism ring[15] $\mathfrak{A}$ of $\mathfrak{M}$, which is considered as right operator-domain, the commuter ring $V(\mathfrak{R})=V_{\mathfrak{A}}(\mathfrak{R})$ of $\mathfrak{R}$ in $\mathfrak{A}$ is nothing but the operator-endomorphism ring of the $\mathfrak{R}$-module $\mathfrak{M}$, we obtain from the above statements, combined with Theorem 2, the following results:

Theorem 3. *Let $\mathfrak{A}$ be an absolute endomorphism ring of a module $\mathfrak{M}$ and suppose that there be given a (primary) uni-serial subring $\mathfrak{R}$ of $\mathfrak{A}$. Then*

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

2) *Every automorphism of $\mathfrak{R}$ can be extended to an inner automorphism of $\mathfrak{A}$.*

3) *In case $\mathfrak{M}$ is regular with respect to $\mathfrak{R}$, any isomorphism τ of $\mathfrak{R}$ into $\mathfrak{A}$, such that $\mathfrak{M}$ is regular with respect to $\mathfrak{R}^{\tau}$ and moreover $[\mathfrak{M}\mid\mathfrak{R}]=[\mathfrak{M}\mid\mathfrak{R}^{\tau}]$, can be extended to an inner automorphism of $\mathfrak{A}$.*

4) *$\mathfrak{M}$ is finite and regular with respect to $\mathfrak{R}$ if and only if $V(\mathfrak{R})$ is primary (and hence uni-serial).*[16] *In this case, we have*

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

We prove only the first half of 4), where the "only if" part is obvious. Let $1=e_1+e_2+\cdots\cdots+e_n$ be a decomposition of the unit element into mutually orthogonal and mutually isomorphic primitive idempotent elements in the primary ($\mathfrak{R}$-endomorphism) ring $V(\mathfrak{R})$ of $\mathfrak{M}$. Then $\mathfrak{M}=\mathfrak{M}e_1+\mathfrak{M}e_2+\cdots\cdots+\mathfrak{M}e_n$ gives a direct decomposition of $\mathfrak{M}$ into mutually operator-isomorphic directly indecomporable $\mathfrak{R}$-submoduli, which are necessarily operator-isomor-

---

13) If in particular $\mathfrak{R}$ is simple, every $\mathfrak{R}$-right-module is necessarily regular and we need not the notion of regularity.

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

15) That is, the totality of all homomorphisms of $\mathfrak{M}$ into itself.

16) Asano [1], Satz 8.

phic with (the directly indecomposable direct summand right ideal) $e\mathfrak{R}$ (of $\mathfrak{R}$).

Theorem 4. *Let $\mathfrak{M}$, $\mathfrak{A}$, $\mathfrak{R}$ be as in the preceding theorem and let $\mathfrak{S}$ be a (primary) uni-serial subring of $\mathfrak{R}$. If $\mathfrak{M}$ is regular with respect to $\mathfrak{R}$, then $\mathfrak{M}$ is regular with respect to $\mathfrak{S}$ if and only if $\mathfrak{R}$ is (right-)regular with respect to $\mathfrak{S}$; further $[\mathfrak{M} \mid \mathfrak{R}]$ is finite if and only if both $[\mathfrak{M} \mid \mathfrak{R}]$ and $[\mathfrak{R} \mid \mathfrak{S}]$ are so. And, when this is the case,*

1) *Any isomorphism τ of $\mathfrak{R}$ into $\mathfrak{A}$ which maps $\mathfrak{S}$ onto itself and such that with respect to $\mathfrak{R}^{\tau}$ $\mathfrak{M}$ is also regular can be extended to an inner automorphism of $\mathfrak{A}$.*

2) *Among $\mathfrak{M}$, $V(\mathfrak{S})$ and $V(\mathfrak{R})$ there holds the same situation as among $\mathfrak{M}$, $\mathfrak{R}$ and $\mathfrak{S}$, as above, and moreover*

$$[\mathfrak{R} \mid \mathfrak{S}]\ [V(\mathfrak{R})] = [V(\mathfrak{S}) \mid V(\mathfrak{R})]\ [\mathfrak{S}];$$

in particular $\mathfrak{R}$ possesses linearly independent (right-)basis over $\mathfrak{S}$ 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 from Theorem 3, 3) because $[\mathfrak{M} \mid \mathfrak{R}]\ [e\mathfrak{R} \mid \mathfrak{S}] = [\mathfrak{M} \mid \mathfrak{S}] = [\mathfrak{M} \mid \mathfrak{R}^{\tau}]\ [(e\mathfrak{R})^{\tau} \mid \mathfrak{S}]$ and $[e\mathfrak{R} \mid \mathfrak{S}] = [(e\mathfrak{R})^{\tau} \mid \mathfrak{S}]$ is finite. The first half of 2) is an immediate consequence of Theorem 2, 3), while the second half is readily obtained by eliminating three arguements $[e\mathfrak{R} \mid \mathfrak{S}]$, $[\mathfrak{M} \mid \mathfrak{R}]$ and $[\mathfrak{M} \mid \mathfrak{S}]$ from the following equalities:

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

Corollary.[17] *Let $\mathfrak{R}$ be a uni-serial ring and $\mathfrak{S}$ its uni-serial subring such that $\mathfrak{R}$ is right-regular and finite with respect to $\mathfrak{S}$. Then two $\mathfrak{R}$-right-moduli are operator-isomorphic if and only if they are so with respect to $\mathfrak{S}$.*

§ 3. Uni-serial subalgebras of a simple ring.

Above preparations now enable us to prove the following

Theorem 5.[18] *Let $\mathfrak{R}$ be a simple ring with the center Z and $\mathfrak{S}$ be a (primary) uni-serial subalgebra (of finite rank) over Z and further $\mathfrak{S}$ be*

---

17) This is an equivalent statement with Theorem 4, 1), as a matter of fact.

18) This theorem is a refinement of results in Asano [1], § 5.

the commuter ring of $\mathfrak{T}$ *in* $\mathfrak{R}$: $\mathfrak{S}=V_{\mathfrak{R}}(\mathfrak{T})$. *Then*

1) $V_{\mathfrak{R}}(\mathfrak{S})=\mathfrak{T}$.

2) *Every automorphism of* $\mathfrak{R}$ *which leaves invariant every element of* $\mathfrak{S}$ *is inner.*

3) *The following five conditions are equivalent to each other*[19]:

i) $\mathfrak{R}$ *is right-regular with respect to* $\mathfrak{T}$,

i′) $\mathfrak{R}$ *is left-regular with respect to* $\mathfrak{T}$,

ii) $\mathfrak{S}$ *is (primary) uni-serial,*

iii) $\mathfrak{R}$ *is right-regular with respect to* $\mathfrak{S}$,

iii′) $\mathfrak{R}$ *is left-regular with respect to* $\mathfrak{S}$.

4) *If* $\mathfrak{S}_0$ *is a (primary) uni-serial subring of* $\mathfrak{R}$ *containing* $\mathfrak{S}$, *then* $V_{\mathfrak{R}}(V_{\mathfrak{R}}(\mathfrak{S}_0))=\mathfrak{S}_0$. *Hence, in particular, uni-serial subalgebras* $\mathfrak{T}_0$ *of* $\mathfrak{T}$ *with respect to which* $\mathfrak{R}$ *is regular and uni-serial subrings* $\mathfrak{S}_0$ *between* $\mathfrak{R}$ *and* $\mathfrak{S}$ *with respect to which* $\mathfrak{R}$ *is regular are in one-to-one correspondence by the commuter relation in* $\mathfrak{R}$: $V_{\mathfrak{R}}(\mathfrak{T}_0)=\mathfrak{S}_0$, $V_{\mathfrak{R}}(\mathfrak{S}_0)=\mathfrak{T}_0$.

5) *If* $\mathfrak{R}$ *is regular with respect to* $\mathfrak{T}$, *then* $\mathfrak{R}$ *possesses a linearly independent (right and left) basis over* $\mathfrak{S}$ *and moreover* $[\mathfrak{R}:\mathfrak{S}]=[\mathfrak{T}:Z]$. *Further, there exists an element* b *in* $\mathfrak{R}$ *such that for any linearly independent basis* $a_1, a_2, \ldots\ldots, a_n$ *of* $\mathfrak{T}$ *over* Z $(: n=[\mathfrak{T}:Z])$, $a_1b, a_2b, \ldots\ldots, a_nb$ *and* $ba_1, ba_2, \ldots\ldots, ba_n$ *form respectively a linearly independent right- and left-basis of* $\mathfrak{R}$ *over* $\mathfrak{S}$; *in other words, the regular representation*[20] *of* $\mathfrak{T}$ *(in* Z*) is equivalent with the representation of* $\mathfrak{T}$ *in* $\mathfrak{S}$ *which is obtained by the* ($\mathfrak{S}$-$\mathfrak{T}$- *or* $\mathfrak{T}$-$\mathfrak{S}$-) *representation module* $\mathfrak{R}$.

6) *In case* $\mathfrak{R}$ *is regular with respect to* $\mathfrak{T}$, *there exists between right* [*left*] *ideals* $\mathfrak{r}$ *of* $\mathfrak{R}$ *which are left-*[*right-*] *allowable with respect to* $\mathfrak{S}$ *and right* [*left*] *ideals*[20] $\mathfrak{t}$ *of* $\mathfrak{T}$ *a one-to-one correspondence by the following relation:*

$$\mathfrak{r}=\mathfrak{t}\mathfrak{R}\ [\mathfrak{r}=\mathfrak{R}\mathfrak{t}],\quad \mathfrak{t}=\mathfrak{r}\frown\mathfrak{T}.$$

The same also holds between right [*left*] *ideals of* $\mathfrak{R}$ *left-*[*right-*]*allowable with respect to* $\mathfrak{T}$ *and right* [*left*] *ideals of* $\mathfrak{S}$.

7) *In case* $\mathfrak{R}$ *is regular with respect to* $\mathfrak{T}$, *any isomophism* τ *of* $\mathfrak{T}$ *into* $\mathfrak{R}$ *leaving* Z *element-wise fixed such that* $\mathfrak{R}$ *is regular with respect to* $\mathfrak{T}^{\tau}$ *can*

---

19) Further $\mathfrak{S}$ is simple if simple if and only if $\mathfrak{T}$ is so.

20) Since every uni-serial algebra is Frobeniusean, its right and left regular representations are equivalent to each other and moreover its right and left ideal lattices are dual-isomorphic to each other (by annihilation relation). See Nakayama [10].

be extended to an inner automorphism of $\mathfrak{R}$.

Proof. Consider the absolute endomorphism ring $\mathfrak{A}$ of $\mathfrak{R}$. By right-sided multiplication each element of $\mathfrak{R}$ induces on $\mathfrak{R}$ an absolute endomorphism and their totality forms a subring of $\mathfrak{A}$ isomorphic with $\mathfrak{R}$, which we shall denote also by $\mathfrak{R}$. Similarly, by left-sided multiplication there is obtained a subring $\mathfrak{R}'$ of $\mathfrak{A}$ inverse-isomorphic with $\mathfrak{R}$. They are, as is well known, commuter rings to each other and hence their intersection $\mathfrak{R}\frown\mathfrak{R}'$ coincides with their common center Z.

According to Theorem 1, the product ring $\mathfrak{T}\mathfrak{R}'$ of $\mathfrak{T}$ and $\mathfrak{R}'$ (constructed in $\mathfrak{A}$) is in fact direct (over Z): $\mathfrak{T}\mathfrak{R}'=\mathfrak{T}\times\mathfrak{R}'$, and moreover its two-sided ideals and two-sided ideals of $\mathfrak{T}$, correspond one-to-one, and this implies that $\mathfrak{T}\times\mathfrak{R}'$ is uni-serial. Hence by Theotem 3, 1)

$$V(V(\mathfrak{T}\times\mathfrak{R}'))=\mathfrak{T}\times\mathfrak{R}'.$$

But since

$$\mathfrak{S}=V_{\mathfrak{R}}(\mathfrak{T})=V(\mathfrak{T})\frown\mathfrak{R}=V(\mathfrak{T})\frown V(\mathfrak{R}')=V(\mathfrak{T}\times\mathfrak{R}'),$$

we obtain

$$V_{\mathfrak{R}}(\mathfrak{S})=V(\mathfrak{S})\frown\mathfrak{R}=V(V(\mathfrak{T}\times\mathfrak{R}'))\frown V(\mathfrak{R}')=(\mathfrak{T}\times\mathfrak{R}')\frown V(\mathfrak{R}')=\mathfrak{T}.$$

To prove 2), let σ be any automorphism of $\mathfrak{R}$ which leaves invariant every element of $\mathfrak{S}$. Regarding σ as an element of $\mathfrak{A}$, it must belong to $V(\mathfrak{S})=\mathfrak{T}\times\mathfrak{R}'$ since $a\sigma=\sigma a^{\sigma}$ holds for every $a\in\mathfrak{R}$. σ satisfies also $a'\sigma=\rho(a')^{\sigma}$ for every $a'\in\mathfrak{R}'$ and hence σ is, by Theorem 1, 3), inner in ($\mathfrak{R}'$ whence) $\mathfrak{R}$.

Since $V(\mathfrak{T}\times\mathfrak{R}')=\mathfrak{S}$, $V(\mathfrak{S})=\mathfrak{T}\times\mathfrak{R}'$ and $\mathfrak{R}$ is finite with respect to ($\mathfrak{R}'$ whence) $\mathfrak{T}\times\mathfrak{R}'$, Theorem 2, 3) shows that $\mathfrak{R}$ is (right-)regular with respect to $\mathfrak{T}\times\mathfrak{R}'$ if and only if $\mathfrak{R}$ is (right-) egular with respect to $\mathfrak{S}$, while Theorem 3, 4) asserts that this holds if and only if $\mathfrak{S}$ is primary (uni-serial). On the other hand, since $\mathfrak{T}\times\mathfrak{R}'$ possesses a linearly independent basis over $\mathfrak{T}$ and there exists a one-to-one correspondence between two-sided ideals of $\mathfrak{T}\times\mathfrak{R}'$ and $\mathfrak{T}$, $\mathfrak{R}$ is (right-)regular with respect to $\mathfrak{T}\times\mathfrak{R}'$ if and only if $\mathfrak{R}$ is (right)regular with respect to $\mathfrak{T}$. Observing further that the primarity of $\mathfrak{S}$ is a condition of the left-right symmetry, we complete the proof of 3).

Consider now a uni-serial subriug $\mathfrak{S}_0$ of $\mathfrak{R}$ which contains $\mathfrak{S}$. Then $V(\mathfrak{S}_0)$ lies necessarily between $V(\mathfrak{R})=\mathfrak{R}'$ and $V(\mathfrak{S})=\mathfrak{T}\times\mathfrak{R}'$ and so, if we put $\mathfrak{T}_0=\mathfrak{T}\frown V(\mathfrak{S}_0)=V_{\mathfrak{R}}(\mathfrak{S})\frown V(\mathfrak{S}_0)=V_{\mathfrak{R}}(\mathfrak{S}_0)$, we have, in virtue of Theorem 1, 2), $V(\mathfrak{S}_0)=\mathfrak{T}_0\times\mathfrak{R}'$. Since $\mathfrak{S}_0$ is uni-serial, it follows $\mathfrak{S}_0=V(V(\mathfrak{S}_0))$

$= V(\mathfrak{T}_0 \times \mathfrak{R}') = V(\mathfrak{T}_0) \frown V(\mathfrak{R}') = V_{\mathfrak{R}}(\mathfrak{T}_0)$. This proves 4).

Assume, from now on, that $\mathfrak{R}$ is regular with respect to $\mathfrak{T}$. Since every (linearly independent) basis of $\mathfrak{T}$ over Z is at the same that of $\mathfrak{T} \times \mathfrak{R}'$ over $\mathfrak{R}'$, the first part of 5) follows from Theorem 4, 2); the existence of left-basis is a consequence of the left-right symmetry. Since $\mathfrak{T} \times \mathfrak{R}'$ is operator-isomorphic to the n-times direct sum of $\mathfrak{R}$ as $\mathfrak{R}'$-(right-)module, they are, by Corollary to Theorem 4, operator-isomorphic even as $\mathfrak{T} \times \mathfrak{R}'$-whence $\mathfrak{T} \times \mathfrak{S}'$-(right-)module; $\mathfrak{S}'$ being the subring of $\mathfrak{R}'$ corresponding to $\mathfrak{S}$. On the other hand, since every linearly independent (right-)basis of $\mathfrak{R}'$ over $\mathfrak{S}'$ is at the same that of $\mathfrak{T} \times \mathfrak{R}'$ over $\mathfrak{T} \times \mathfrak{S}'$, $\mathfrak{T} \times \mathfrak{R}'$ is, as $\mathfrak{T} \times \mathfrak{S}'$-(right-)module, operator-isomorphic to the n-times direct sum of $\mathfrak{T} \times \mathfrak{S}'$. Hence $\mathfrak{R}$ and $\mathfrak{T} \times \mathfrak{S}'$[21] are, by Krull-Remak-Schmidt theorem, operator-isomorphic as $\mathfrak{T} \times \mathfrak{S}'$-module. Now let b be the element of $\mathfrak{R}$ corresponding to the unit element of $\mathfrak{T} \times \mathfrak{S}'$. Then, since $V(\mathfrak{T} \times \mathfrak{S}') = V(\mathfrak{T}) \frown V(\mathfrak{S}') = V(\mathfrak{T}) \frown (\mathfrak{R} \times \mathfrak{T}') = \mathfrak{S} \times \mathfrak{T}'$, there is, by Lemma 3, an $\mathfrak{S} \times \mathfrak{T}'$-isomorphism between $\mathfrak{R}$ and $\mathfrak{S} \times \mathfrak{T}'$ in which b corresponds also to the unit element of $\mathfrak{S} \times \mathfrak{T}'$. This shows that b is the desired element in the second part of 5).

Every left ideal of $\mathfrak{T} \times \mathfrak{R}'$ which is right-allowable with respect to $\mathfrak{R}'$ is, in virtue of Theorem 1, 2), expressed as $\mathfrak{t} \times \mathfrak{R}'$ by a (uniquely determined) left ideal $\mathfrak{t}$ of $\mathfrak{T}$ and therefore every $\mathfrak{S}$-$\mathfrak{R}'$-submodule of $\mathfrak{R}$ is, according to Theorem 2, 1), of the form $\mathfrak{R} \cdot (\mathfrak{t} \times \mathfrak{R}') = \mathfrak{R}\mathfrak{t}$. This proves the first half of 6). The proof of the second half is obtained by using Theorem 3 and is rather simple.

As for 7), the isomorphism τ can be extended in a natural manner to an isomorphism between $\mathfrak{T} \times \mathfrak{R}'$ and $\mathfrak{T}^{\tau} \times \mathfrak{R}'$ which leaves $\mathfrak{R}'$ element-wise invariant. Then Theorem 4, 1) implies that there is a regular element a in $\mathfrak{A}$ such that $a^{-1}xa = x^{\tau}$ for every $x \in \mathfrak{T}$ and moreover a is elementwise commutative with $\mathfrak{R}'$; but the latter condition means that a (and a^{-1}) belong to $V(\mathfrak{R}') = \mathfrak{R}$. The proof is thus completed.

§ 4. Galois theory for uni-serial rings (in the sense of Jacobson).

Let $\mathfrak{R}$ be first any ring and σ its arbitrary automorphism. If we difine, for any pair of elements a, x of $\mathfrak{R}$, a new product $a * x$ by

---

21) The $\mathfrak{S}$-$\mathfrak{T}$-module $\mathfrak{T} \times \mathfrak{S}'$ intermediates the regular representation of $\mathfrak{T}$, as can easily be seen.

$$a*x = a^{\sigma}x,$$

then $\mathfrak{R}$ becomes a new $\mathfrak{R}$-left-module and moreover, if the right-sided multiplication is taken as the original one, $\mathfrak{R}$ is considered as an $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, which we shall denote by $(\mathfrak{R}, \sigma)$[22]. We may readily prove

Lemma 4.[22] *$(\mathfrak{R}, \sigma)$ and $(\mathfrak{R}, \tau)$ are operator-isomorphic, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-moduli, if and only if the automorphism $\sigma\tau^{-1}$ is inner (in $\mathfrak{R}$).*

Now let $\mathfrak{R}$ be (primary) uni-serial and $\mathfrak{C}$ its radical having exponent l and put $\bar{\mathfrak{R}} = \mathfrak{R}/\mathfrak{C}$. $\mathfrak{C}$ is a principal two-sided ideal generated by a single element c; $\mathfrak{C} = \mathfrak{R}c = c\mathfrak{R}$. If we associate with each $x \in \mathfrak{R}$ the element $y \in \mathfrak{R}$ such that $xc \equiv cy \pmod{\mathfrak{C}^2}$, we obtain, since $x\mathfrak{C} \subseteqq \mathfrak{C}^2$ $[\mathfrak{C}y \subseteqq \mathfrak{C}^2]$ is equivalent to $x \in \mathfrak{C}$ $[y \in \mathfrak{C}]$, an automorphism of the simple ring $\bar{\mathfrak{R}}$, which we shall denote by φ[23]. $\mathfrak{C}/\mathfrak{C}^2$ is then operator-isomorphic, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, with $(\bar{\mathfrak{R}}, \varphi)$; hence φ is, by Lemma 4, uniquely determined up to inner automorphism of $\bar{\mathfrak{R}}$. Since $\mathfrak{C}^i = \mathfrak{R}c^i = c^i\mathfrak{R}$ and moreover $x\mathfrak{C}^i \subseteqq \mathfrak{C}^{i+1}$ $[\mathfrak{C}^i y \subseteqq \mathfrak{C}^{i+1}]$ if and only if $x \in \mathfrak{C}$ $[y \in \mathfrak{C}]$ for each $i = 1, 2, \ldots\ldots, l-1$, $\mathfrak{C}^i/\mathfrak{C}^{i+1}$ is operator-isomorphic to $(\bar{\mathfrak{R}}, \varphi^i)$. Now every automorphism σ of $\mathfrak{R}$ induces naturally an automorphism in $\bar{\mathfrak{R}}$, which will be denoted also by σ. Then, since $\mathfrak{C} = \mathfrak{C}^{\sigma} = \mathfrak{R}c^{\sigma} = c^{\sigma}\mathfrak{R}$, necessarily

$$\sigma\varphi \equiv \varphi\sigma,$$

where $\equiv$ means the congruence modulo the totality of inner automorphisms of $\bar{\mathfrak{R}}$.

Suppose now that there is given a finite group $\mathfrak{G} = \{1, \sigma, \ldots\ldots, \tau\}$ of automorphism of $\mathfrak{R}$ each element σ of which satisfies the following condition:

(*)[24] *If $\sigma \neq 1$ then $\sigma \not\equiv \varphi^i$ for any $i = 0, 1, 2, \ldots\ldots, l-1$.*

Then we can define a *crossed product* $(\mathfrak{R}, \mathfrak{G})$ of $\mathfrak{R}$ by $\mathfrak{G}$ as follows:

$(\mathfrak{R}, \mathfrak{G})$ is a ring containing $\mathfrak{R}$ as a subring and with each $\sigma \in \mathfrak{G}$ there is associated a regular element u_σ of $(\mathfrak{R}, \mathfrak{G})$ such that

$$(\mathfrak{R}, \mathfrak{G}) = u_1\mathfrak{R} \smile u_\sigma\mathfrak{R} \smile \ldots\ldots \smile u_\tau\mathfrak{R}, \quad xu_\sigma = u_\sigma x^\sigma \ (x \in \mathfrak{R}).$$

Then we prove

22) Cf. Azumaya, [3], § 2.

23) In case the center of $\mathfrak{R}$ is not a field, it contains a nilpotent element $d \neq 0$. Then the two-sided ideal $d\mathfrak{R}$ is of a form $\mathfrak{C}^i$, where $1 \leq i \leq l-1$, and accordingly we have $\varphi^i \equiv 1$. In the contrary case, it may happen that $\varphi^l \not\equiv 1$.

24) In case $\mathfrak{R}$ is commutative, this condition means simply:

If $\sigma \neq 1$ then σ is not identity in $\bar{\mathfrak{R}}$ too.

Theorem 6. *$u_1, u_\sigma, \ldots\ldots, u_\tau$ are linearly independent over $\mathfrak{R}$ (on both left- and right-hand sides), and*

1) *$(\mathfrak{R}, \mathfrak{G})$ is a (primary) uni-serial ring*[25] *and between two-sided ideals $\mathfrak{z}^*$ of $(\mathfrak{R}, \mathfrak{G})$ and two-sided ideals $\mathfrak{z}$ of $\mathfrak{R}$ there is a one-to-one correspondence by the following relation:*

$$\mathfrak{z}^* = (\mathfrak{R}, \mathfrak{G})\mathfrak{z} = \mathfrak{z}(\mathfrak{R}, \mathfrak{G}), \quad \mathfrak{z} = \mathfrak{z}^* \frown \mathfrak{R}.$$

Further, every left [right] ideal of $(\mathfrak{R}, \mathfrak{G})$ which is right-[left-]allowable with respect to $\mathfrak{R}$ is necessarily a two-sided ideal.

2) *Every subring of $(\mathfrak{R}, \mathfrak{G})$ containing $\mathfrak{R}$ which is right-(or left-)regular with respect to $\mathfrak{R}$ is expressed in the form $(\mathfrak{R}, \mathfrak{H})$ by a suitable subgroup $\mathfrak{H}$ of $\mathfrak{G}$.*

3) *A regular element u of $(\mathfrak{R}, \mathfrak{G})$ satisfies $\mathfrak{R}u = u\mathfrak{R}$ if and only if $u\mathfrak{R} = u_\sigma\mathfrak{R}$ for a suitable σ in $\mathfrak{G}$.*

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

Proof. Each $u_\sigma\mathfrak{R}$ is operator-isomorphic, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, with $(\bar{\mathfrak{R}}, \sigma)$ and hence possesses the composition residue-class-module series $(\bar{\mathfrak{R}}, \sigma), (\bar{\mathfrak{R}}, \sigma\varphi), (\bar{\mathfrak{R}}, \sigma\varphi^2), \ldots\ldots, (\bar{\mathfrak{R}}, \sigma\varphi^{l-1})$, as can easily be seen. That $\mathfrak{G}$ satisfies the condition (*) means therefore, in virtue of Lemma 4, that if $\sigma \neq \tau$ $u_\sigma\mathfrak{R}$ and $u_\tau\mathfrak{R}$ have no composition residue class module in common. From this follows that $(\mathfrak{R}, \mathfrak{G})$ is indeed a direct sum of $u_1\mathfrak{R}, u_\sigma\mathfrak{R}, \ldots\ldots, u_\tau\mathfrak{R}$ and moreover every $\mathfrak{R}$-$\mathfrak{R}$-submodule of $(\mathfrak{R}, \mathfrak{G})$ is expressed in the form

$$(1) \qquad \sum_\sigma u_\sigma \mathfrak{z}_\sigma,$$

where $\mathfrak{z}_\sigma$ is, for each $\sigma \in \mathfrak{G}$, a two-sided ideal of $\mathfrak{R}$[26].

(1) forms a left ideal of $(\mathfrak{R}, \mathfrak{G})$ i.e. left-allowable with respect to every u_σ if and only if $\mathfrak{z}_1 = \mathfrak{z}_\sigma = \ldots\ldots = \mathfrak{z}_\tau$, that is, (1) is of the form $(\mathfrak{R}, \mathfrak{G})\mathfrak{z}$ by a certain two-sided ideal $\mathfrak{z}$ of $\mathfrak{R}$. Further, since $\mathfrak{z} = \mathfrak{z}^\sigma$ for every $\sigma \in \mathfrak{G}$[27], we have $(\mathfrak{R}, \mathfrak{G})\mathfrak{z} = \mathfrak{z}(\mathfrak{R}, \mathfrak{G})$. And 1) is proved.

Consider now a regular element u of $(\mathfrak{R}, \mathfrak{G})$ such that $\mathfrak{R}u = u\mathfrak{R}$. Then

---

25) This may be seen as a generalization of Nakayama [9], Hilfssatz 1.

26) Let, generally, a module $\mathfrak{M}$ (with operator-domain) be a sum of (allowable) submoduli $\mathfrak{M}_1, \mathfrak{M}_2, \ldots\ldots$ each of which possesses a composition series and such that if $i \neq j$ $\mathfrak{M}_i$ and $\mathfrak{M}_j$ have no composition residue class module in common. Then $\mathfrak{M}$ is indeed direct sum of them and every (allowable) submodule $\mathfrak{N}$ of $\mathfrak{M}$ is expressed in the form $\mathfrak{N} = \mathfrak{N}_1 + \mathfrak{N}_2 + \ldots\ldots$, where $\mathfrak{N}_1, \mathfrak{N}_2, \ldots\ldots$ are submoduli of $\mathfrak{M}_1, \mathfrak{M}_2, \ldots\ldots$ respectively.

27) Because $\mathfrak{z}$ coincides with some $\mathfrak{C}^i$.

since $\mathfrak{R}$ is primary whence is two-sided directly indecomposable, the $\mathfrak{R}$-$\mathfrak{R}$-two-sided module $u\mathfrak{R}$ is also directly indecomposable and hence is contained in one of $u_\sigma\mathfrak{R}$'s. Comparing further the composition lengths, we have indeed $u\mathfrak{R}=u_\sigma\mathfrak{R}$ for some $\sigma\in\mathfrak{G}$. In particular, we have $u_\sigma u_\tau\mathfrak{R}=u_{\sigma\tau}\mathfrak{R}$[28] for any automorphism σ, τ in $\mathfrak{G}$, because $xu_\sigma u_\tau(=u_\sigma x^\sigma u_\tau)=u_\sigma u_\tau x^{\sigma\tau}$ for every $x\in\mathfrak{R}$. Combining this with the fact that (1) is right-regular with respect to $\mathfrak{R}$ if and only if $\mathfrak{z}_\sigma=\mathfrak{R}$ or $\mathfrak{z}_\sigma=0$, we can readily verify the validity of 2).

Take finally any commuter $\sum_\sigma u_\sigma a_\sigma$ of $\mathfrak{R}$ in $(\mathfrak{R}, \mathfrak{G})$. Then $\sum_\sigma u_\sigma a_\sigma x =x\sum_\sigma u_\sigma a_\sigma=\sum_\sigma u_\sigma x^\sigma a_\sigma$ whence $a_\sigma x=x^\sigma a_\sigma$ for every $x\in\mathfrak{R}$ and $\sigma\in\mathfrak{G}$. This implies however that the two-sided ideal $\mathfrak{R}a_\sigma=a_\sigma\mathfrak{R}$ of $\mathfrak{R}$ is, for each $\sigma\in\mathfrak{G}$, operator-homomorphic to $(\mathfrak{R}, \sigma^{-1})$. It follows from this, since if $\sigma\neq 1$ $\mathfrak{R}=(\mathfrak{R}, 1)$ and $(\mathfrak{R}, \sigma^{-1})$ possess as above no composition residue class module in common, that $a_\sigma=0$ unless $\sigma=1$. Hence the commuter $\sum_\sigma u_\sigma a_\sigma=u_1a_1$ belongs necessarily to the center of $\mathfrak{R}$.

Now we obtain

Theorem 7. *Let $\mathfrak{R}$ be a (primary) uni-serial ring and let $\mathfrak{G}=\{1, \sigma, \ldots\ldots, \tau\}$ be a finite group of its automorphisms whose elements satisfy the condition (*) above. Then*

1) *The subring $\mathfrak{S}$ which belongs to $\mathfrak{G}$, that is, the subring consisting of all elements of $\mathfrak{R}$ which remain invariant under every automorphism in $\mathfrak{G}$ is (primary) uni-serial and two-sided ideals $\mathfrak{a}$ of $\mathfrak{R}$ and two-sided ideals $\mathfrak{b}$ of $\mathfrak{S}$ correspond one-to-one by the following relation:*

$$\mathfrak{a}=\mathfrak{R}\mathfrak{b}=\mathfrak{b}\mathfrak{R},\quad \mathfrak{b}=\mathfrak{a}\frown\mathfrak{S}.$$

Moreover every left [right] ideal of $\mathfrak{R}$ which is right-[left-]allowable with respect to $\mathfrak{S}$ is necessarily a two-sided ideal.

2) *Any automorphism of $\mathfrak{R}$ which leaves invariant every element of $\mathfrak{S}$ is in $\mathfrak{G}$.*

3) *The commuter ring of $\mathfrak{S}$ in $\mathfrak{R}$ coincides with the center of $\mathfrak{R}$.*

4) *$\mathfrak{R}$ possesses a (linearly independent) basis over $\mathfrak{S}$ and $[\mathfrak{R}:\mathfrak{S}]=(\mathfrak{G}:1)$, at both left- and right-hand sides. Furthermore $\mathfrak{R}$ has a left (or right) normal basis over $\mathfrak{S}$, or what is the same, the regular representation of $\mathfrak{G}$ is equivalent with the representation of $\mathfrak{G}$ in $\mathfrak{S}$ which is obtained by the*

28) This means the existence of regular elements $a_{\sigma,\tau}$ in the center of such that $u_\sigma u_\tau=u_{\sigma\tau}a_{\sigma,\tau}$; they form the so-called factorset of $(\mathfrak{R}, \mathfrak{G})$. Further, it is to be noticed that $u_1\mathfrak{R}$ coincides with $\mathfrak{R}$.

$\mathfrak{S}$-$\mathfrak{G}$-(*or* $\mathfrak{G}$-$\mathfrak{S}$-) *representation module* $\mathfrak{R}$; *If in particular* $\mathfrak{G}$ *is abelian, then every left* [*right*] *normal basis is at the same time a right* [*left*] *normal basis.*

5) *Any subring of* $\mathfrak{R}$ *which contains* $\mathfrak{S}$ *and with respect to which* $\mathfrak{R}$ *is right- or left-regular belongs to a suitable subgroup* $\mathfrak{H}$ *and hence is* (*primary*) *uni-serial.*

Proof. Consider again the absolute endomorphism ring $\mathfrak{A}$ of $\mathfrak{R}$ and define in it two subrings $\mathfrak{R}$ and $\mathfrak{R}'$ as in the proof of Theorem 5. Looking upon each $\sigma\in\mathfrak{G}$ as an element of $\mathfrak{A}$, we have

(2) $$x'\sigma=\sigma(x')^{\sigma} \text{ for every } x'\in\mathfrak{R}'$$

and hence $\mathfrak{R}'\smile\sigma\mathfrak{R}'\smile\ldots\ldots\smile\tau\mathfrak{R}'$ forms a crossed product $(\mathfrak{R}', \mathfrak{G})$. Since each $\sigma\in\mathfrak{G}$ satisfies the condition (*) for $\mathfrak{R}'$, it follows from Theorem 6, 1) that $(\mathfrak{R}', \mathfrak{G})$ is uni-serial and indeed its two-sided ideals and two-sided ideals of $\mathfrak{R}'$ correspond one-to-one in the usual manner. These imply that $\mathfrak{R}$ is (right-)regular and finite with respect to $(\mathfrak{R}', \mathfrak{G})$. Now the subring $\mathfrak{S}$ belonging to $\mathfrak{G}$ is, because of (2), nothing but the commuter ring of $(\mathfrak{R}', \mathfrak{G})$ in $\mathfrak{A}$: $\mathfrak{S}=V(\mathfrak{R}', \mathfrak{G})$. Hence $\mathfrak{S}$ is, according to the Theorem 3, (primary) uni-serial and $V(\mathfrak{S})=(\mathfrak{R}', \mathfrak{G})$. Let $\mathfrak{a}'$ be any two-sided ideal of $\mathfrak{R}'$. Then $(\mathfrak{R}', \mathfrak{G})\mathfrak{a}'$ forms a two-sided ideal of $(\mathfrak{R}', \mathfrak{G})$ and there corresponds, by Corollary to Theorem 2, a (uniquely determined) two-sided ideal $\mathfrak{b}$ of $\mathfrak{S}$ such that $\mathfrak{R}\mathfrak{b}=\mathfrak{R}\cdot\mathfrak{R}(\mathfrak{R}', \mathfrak{G})\mathfrak{a}'=\mathfrak{a}$ and $\mathfrak{b}=\mathfrak{a}\frown\mathfrak{S}$; by the left-right symmetry we should also have $\mathfrak{b}\mathfrak{R}=\mathfrak{a}$. Conversely take any two-sided ideal $\mathfrak{b}$ of $\mathfrak{S}$. Then again by Corollary to Theorem 2 there exists a two-sided ideal which we may write according to Theorem 6, 1) $(\mathfrak{R}', \mathfrak{G})\mathfrak{a}'$ with a two-sided ideal $\mathfrak{a}'$ of $\mathfrak{R}'$ such that $\mathfrak{R}\mathfrak{b}=\mathfrak{R}\cdot(\mathfrak{R}', \mathfrak{G})\mathfrak{a}'=\mathfrak{a}$. This implies that $\mathfrak{R}\mathfrak{b}$ is a two-sided ideal of $\mathfrak{R}$ and hence $\mathfrak{R}\mathfrak{b}=\mathfrak{b}\mathfrak{R}$. Further since every left ideal of $(\mathfrak{R}', \mathfrak{G})$ which is right-allowable with respect to $\mathfrak{R}'$ is also expressed in the form $(\mathfrak{R}', \mathfrak{G})\mathfrak{z}'$ by a certain two-sided ideal $\mathfrak{z}'$ of $\mathfrak{R}'$, every left ideal of $\mathfrak{R}$ which is right-allowable with respect to $\mathfrak{S}$ is, in virtue of Theorem 2, 1), of the form $\mathfrak{R}\cdot(\mathfrak{R}', \mathfrak{G})\mathfrak{z}'=\mathfrak{z}$ and so is a two-sided ideal of $\mathfrak{R}$. Thus 1) is proved.

To prove 2), let ρ be any automorphism of $\mathfrak{R}$ under which every element of $\mathfrak{S}$ remains invariant. Then since $x\rho=\rho x^{\rho}$ for every $x\in\mathfrak{R}(\subseteq\mathfrak{A})$, ρ being considered as an element of $\mathfrak{A}$, ρ lies necessarily in $V(\mathfrak{S})=(\mathfrak{R}', \mathfrak{G})$. Since further $x'\rho=\rho(x')^{\rho}$ for every $x'\in\mathfrak{R}'$ ρ satisfies $\mathfrak{R}'\rho=\rho\mathfrak{R}'$ and therefore $\rho\mathfrak{R}'$ coincides, according to Theorem 6, 3), with a certain $\sigma\mathfrak{R}'$, that is, there exists an automorphism σ in $\mathfrak{G}$ and a regular element c' in $\mathfrak{R}'$ such that $\rho=\sigma c'$. Then $x^{\rho}=\rho^{-1}x\rho=(c')^{-1}\sigma^{-1}x\sigma c'=(c')^{-1}x^{\sigma}c'=x^{\sigma}$ for every $x\in\mathfrak{R}$ and hence we have $\rho=\sigma\in\mathfrak{G}$.

3) is a direct consequence of Theorem 6, 4) since $V_{\mathfrak{R}}(\mathfrak{S})=\mathfrak{R}\frown V(\mathfrak{S})=V(\mathfrak{R}')\frown(\mathfrak{R}', \mathfrak{G})$ and the center of $\mathfrak{R}'$ coincides with that of $\mathfrak{R}$.

That $(\mathfrak{R}', \mathfrak{G})$ has the linearly independent basis $1, \sigma, \ldots\ldots, \tau$ over $\mathfrak{R}'$ implies, in virtue of Theorem 4, 2), the first half of 4); the existence of left basis (of $\mathfrak{R}$ over $\mathfrak{S}$) is a consequence of the left-right symmetry. That implies also $(\mathfrak{R}', \mathfrak{G})$ is operator-isomorphic to the n-times direct sum of $\mathfrak{R}$ with respect to the right operator-ring $\mathfrak{R}'$, n being the order of $\mathfrak{G}$, and therefore they are operator-isomorphic, by Corollary to Theorem 4, even with respect to $(\mathfrak{R}', \mathfrak{G})$ whence with respect to $(\mathfrak{S}', \mathfrak{G})$. On the other hand, since every right-basis of $\mathfrak{R}'$ over $\mathfrak{S}'$ is at the same time that of $(\mathfrak{R}', \mathfrak{G})$ over $(\mathfrak{S}', \mathfrak{G})$, $(\mathfrak{R}', \mathfrak{G})$ is operator-isomorphic to the n-times direct sum of $(\mathfrak{S}', \mathfrak{G})$ with respect to (the right operator-ring) $(\mathfrak{S}', \mathfrak{G})$. From these follows by Krull-Remak-Schmidt theorem that $\mathfrak{R}$ is, as $(\mathfrak{S}', \mathfrak{G})$-right-module, operator-isomorphic to $(\mathfrak{S}', \mathfrak{G})$. Let b be then the element of $\mathfrak{R}$ which corresponds to the unit element of $(\mathfrak{S}', \mathfrak{G})$, the group ring of $\mathfrak{G}$ over $\mathfrak{S}'$. Then $b, b^{\sigma}, \ldots\ldots, b^{\tau}$ form a desired left normal basis of $\mathfrak{R}$ over $\mathfrak{S}$. If in particular $\mathfrak{G}$ is abelian, then $V(\mathfrak{S}', \mathfrak{G})=V(\mathfrak{S}')\frown V(\mathfrak{G})=(\mathfrak{R}, \mathfrak{G})\frown V(\mathfrak{G})=(\mathfrak{S}, \mathfrak{G})$ and hence there exists by Lemma 3 an $(\mathfrak{S}, \mathfrak{G})$-isomorphism between $\mathfrak{R}$ and $(\mathfrak{S}, \mathfrak{G})$ in which b corresponds to the unit element of $(\mathfrak{S}, \mathfrak{G})$, that is, $b, b^{\sigma}, \ldots\ldots, b^{\tau}$ form also a right normal basis of $\mathfrak{R}$ over $\mathfrak{S}$. Thus 4) is proved.

To prove 5) let $\mathfrak{T}$ be a subring of $\mathfrak{R}$ containing $\mathfrak{S}$ such that $\mathfrak{R}$ is regular with respect to it. Theorem 4 implies then that $V(\mathfrak{T})$ is regular with respect to its subring $\mathfrak{R}'$ and moreover $V(V(\mathfrak{T}))=\mathfrak{T}$. From the first statement follows according to Theorem 6, 2) that $V(\mathfrak{T})$ is, for a suitable subgroup $\mathfrak{H}$ of $\mathfrak{G}$, expressed as $(\mathfrak{R}', \mathfrak{H})$, and so we have, from the second statement, $\mathfrak{T}=V(\mathfrak{R}', \mathfrak{H})$, that is, $\mathfrak{T}$ belongs to the subgroup $\mathfrak{H}$.

Remark. Meanwhile Nakayama has shown that our results in this section can be extended further to rings with minimum condition for left and right ideals; this, *the Galois theory for general rings*, will shortly appear in these Journals.

Addendum. In connection with Theorem 1 we may prove the following theorem the first part of which may be considered as a generalization of Theorem 1, 3) as well as Azumaya [3], Lemma 2.

Theorem 8. *Let $\mathfrak{R}$ and $\mathfrak{S}$ be two rings both containing a (commutative) field K as a subfield of their center and construct their direct product $\mathfrak{R}\times\mathfrak{S}$ over K. Then*

1) *Under both the maximum and minimum conditions for two-sided ideals in $\mathfrak{R}$, an automorphism of $\mathfrak{R}$ can be extended to an inner automorphism of $\mathfrak{R}\times\mathfrak{S}$ if and only if it is already inner in $\mathfrak{R}$.*

2) *Under the minimum condition for left and right ideals in $\mathfrak{R}$ and the finiteness of the rank $[\mathfrak{S}:K]$, a two-sided ideal $\mathfrak{a}$ of $\mathfrak{R}$ is both left and right principal if and only if the two-sided ideal $\mathfrak{a}\times\mathfrak{S}$ of $\mathfrak{R}\times\mathfrak{S}$ is so.*

Proof. Let $\{b_\nu\}$ be a (linearly independent) basis of $\mathfrak{S}$ over K. Then it forms also a basis of $\mathfrak{R}\times\mathfrak{S}$ over $\mathfrak{R}$. So $\mathfrak{R}\times\mathfrak{S}$ is, as $\mathfrak{R}$-$\mathfrak{R}$-two-sided-module, a direct sum of submoduli $\mathfrak{R}b_\nu=b_\nu\mathfrak{R}$ operator-isomorphic to $\mathfrak{R}$. Suppose that an automorphism σ of $\mathfrak{R}$ can be extended to an inner automorphism of $\mathfrak{R}\times\mathfrak{S}$ which is induced by a regular element u in $\mathfrak{R}\times\mathfrak{S}$: $u^{-1}au=a^\sigma$ $(a\in\mathfrak{R})$. Then $\mathfrak{R}\times\mathfrak{S}=(\mathfrak{R}\times\mathfrak{S})u=\sum\mathfrak{R}b_\nu u$, gives a direct decomposition of $\mathfrak{R}\times\mathfrak{S}$ into submoduli $\mathfrak{R}b_\nu u$ each of which is, since $ab_\nu u=b_\nu au$ $=b_\nu ua^\sigma$ for every $a\in\mathfrak{R}$, operater-isomorphic to $(\mathfrak{R},\sigma)$. Thus we have two direct decompositions of $\mathfrak{R}\times\mathfrak{S}$ into mutually operater-isomorphic submoduli. Owing to the chain condition, $\mathfrak{R}$ can be decomposed into a direct sum of (mutually orthogonal whence) mutually never-operator-isomorphic directly indecomposable two-sided ideals. This decomposition also gives the similar for $(\mathfrak{R},\sigma)$. It follows therefore from Krull-Remak-Schmidt theorem that $\mathfrak{R}=(\mathfrak{R},1)$ is operator-isomorphic to $(\mathfrak{R},\sigma)$, which means according to Lemma 4 that σ is inner in $\mathfrak{R}$.

To prove 2), assume that $\mathfrak{a}\times\mathfrak{S}$ is generated by a single element c of $\mathfrak{R}\times\mathfrak{S}$ on both left- and right-hand sides[29]: $\mathfrak{a}\times\mathfrak{S}=(\mathfrak{R}\times\mathfrak{S})c=c(\mathfrak{R}\times\mathfrak{S})$. Then, since $l(\mathfrak{a})\times\mathfrak{S}$, $l(\mathfrak{a})$ being the left annihilator ideal of $\mathfrak{a}$ in $\mathfrak{R}$, is the left annihilator ideal of $\mathfrak{a}\times\mathfrak{S}$, i.e. of c, in $\mathfrak{R}\times\mathfrak{S}$, $\mathfrak{a}\times\mathfrak{S}$ is operator-isomorphic to $\mathfrak{R}\times\mathfrak{S}/l(\mathfrak{a})\times\mathfrak{S}\cong[\mathfrak{R}/l(\mathfrak{a})]\times\mathfrak{S}$ with respect to the left operator-ring $\mathfrak{R}\times\mathfrak{S}$ whence with respect to $\mathfrak{R}$ too. Hence we have, again by Krull-Remak-Schmidt theorem, that $\mathfrak{a}$ is operator-isomorphic to $\mathfrak{R}/l(\mathfrak{a})$ with respect to (the left operator-ring) $\mathfrak{R}$, which implies that $\mathfrak{a}$ is left principal. Similarly $\mathfrak{a}$ is right principal. The converse is evident.

Remark. After the completion of the present paper, the writer found

29) Cf. Nakamaya [11], Lemma 1.

that many of the results in the present paper as well as in the previous paper Azumaya [2] are, though in the case of simple rings, proved in Artin-Nesbitt-Thrall, "Rings with minimum condition", Michigan Press (1944) by making use of the notion of analytic linear functions; the analytic linear functions of a simple ring $\mathfrak{R}$ are, on retaining the notations in the proof of Theorem 5 of the present paper, nothing but the elements in the subring $\mathfrak{R}\times\mathfrak{R}'$ of $\mathfrak{A}$. We notice here that their Theorem 7.3 H can be proved in a somewhat simpler way if we observe that every subring of $\mathfrak{R}\times\mathfrak{R}'$ containing $\mathfrak{R}'$ is according to our Theorem 1, 2) expressed as $\mathfrak{T}\times\mathfrak{R}'$ by a suitable subring $\mathfrak{T}$ between $\mathfrak{R}$ and Z.[30]

Mathematical Institute,
Nagoya University.

References.

1. K. Asano, Über verallgemeinerte Abelsche Gruppen mit hyperkomplexem operatorenring und ihre Anwendungen, Jap. J. Math. **15** (1939).

2. G. Azumaya, New foundation for the theory of simple rings, forthcoming in Proc. Imp. Acad. Tokyo.

3. G. Azumaya, On almost symmetric algebras, Jap. J. Math. **19** (1948).

4. G. Azumaya, On generalized semi-primary rings and Krull-Remak-Schmidt's theorem, Jap. J. Math. **19** (1947).

5. G. Azumaya and T. Nakayama, On absolutely uni-serial algebras, Jap. J. Math. **19** (1948).

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

7. G. Köthe, Verallgemeinerte Abelsche Gruppe mit hyperkomplexem Operatorring, Math. Zeitschr. **39** (1934).

8. A. Kurosh, Direct decompositions of simple rings, Recueil Math. **53** (1942).

9. T. Nakayama, Über die Klassifikation halblinearer Transformationen, Proc. Phys. Math. Soc. Japan **19** (1937).

10. T. Nakayama, On Frobeniusean algebras, I, Ann. Math. **40** (1939); Ibid., II, Ann. Math. **42** (1941).

11. T. Nakayama, Note on uni-serial and generalized uni-serial rings, Proc. Imp. Acad. Tokyo **16** (1940).

12. T. Nakayama, Normal basis of a quasi-field, Proc. Imp. Acad. Tokyo, **16** (1940).

13. T. Nakayama and G. Azumaya, On irreducible rings, Ann. Math. **48** (1947).

14. E. Noether, Nichtkommutative Algebra, Math. Zeitschr. **39** (1933).

---

30) We also point out that their Theorem 7.3F is already proved essentially in A. A. Albert, Structure of algebras, New York (1939), Theorem 4.6. Cf. also Kurosh [8], Theorem 11.