GALOIS THEORY OF SIMPLE RINGS

BY

TADASI NAKAYAMA

Introduction. The outer Galois theory, started by Jacobson [8], has been developed rather thoroughly [2; 3; 6; 12; 16]. The general Galois theory, dealing with general groups of automorphisms (with some restrictions though), has been established by Cartan [5] and Jacobson [9] in case of sfields. The purpose of the present paper is to offer a similar theory for simple rings with minimum condition (1). The same has been given in fact in Hochschild [7] for simple algebras (finite over their centers). But the method breaks down in the case of general simple rings, infinite over their centers, and a new approach is necessary (2). The writer [14] has recently shown that if \( A \) is a simple ring and \( C \) is a weakly normal (cf. §1 below) simple subring of \( A \), then the \( A \)-left-, \( C \)-right-module \( A \) is fully reducible, and he has applied this fact, together with some methods in Dieudonné [6], to obtain a theorem of extension for isomorphisms in simple rings. It turns out that this full reducibility of \( A \), with respect to the left-multiplication of \( A \) and the right-multiplication of \( C \), and some crossed product theorems, proved and used in the older papers by Azumaya and the writer [3; 12; 13; 16], are appropriate means for establishing the Galois theory (3) for simple rings. In fact, if \( A \) is in particular a sfield, then \( A \) is clearly minimal (= irreducible) with respect to any operator domain containing the left-multiplication ring of \( A \), and this fact underlies the Galois theory, as well as many other theories, for sfields. It is replaced, when \( A \) is a simple ring, by our \( A \)-\( C \)-full reducibility.

The first section of the present paper gives some preliminary, though fundamental, lemmas on weakly normal simple subrings of a simple ring. In §2 we introduce regular groups of automorphisms of a simple ring, which are the class of automorphism groups employed in our Galois theory, and consider their invariant systems. Conversely, we consider in §3 the group of automorphisms leaving a subring, of a certain type, elementwise fixed. The Galois theory follows then in §4. Although our method is rather different, we follow there the pattern of the algebra case in Hochschild [7]. Our theory can

Received by the editors August 6, 1951 and, in revised form, July 2, 1952.

(1) A (non-nilpotent) simple ring with minimum condition will be called in the present paper merely a simple ring, in a somewhat old-fashioned way.

(2) It is true that the method of combining "inner" and "outer" Galois theories applies, in a sense, even in our general case. However, there the outer Galois theory should be that of a certain subring other than the center. The relationship between the automorphisms of the whole ring and such a subring is exactly what produces the difficulty in our general case.

(3) In the present paper the term "Galois theory" is taken in the strict sense as a theory which deals with automorphism groups and their invariant systems.
readily be transferred to the so-called complete primitive rings, and this fact and some other remarks are given in §5.

1. Lemmas. By a ring we mean, throughout this paper, a ring with unit element. By a subring we mean one which contains this unit element. We shall deal only with those modules for which the unit element of our ring is the identity operator. By a simple ring we shall mean a simple ring (with unit element and) with minimum condition. Let $A$ be such a ring, and $r$ be its minimal right-ideal, unique up to isomorphism. $A$ is decomposed into a direct sum $A = r_1 \oplus r_2 \oplus \cdots \oplus r_k$ of minimal right-ideals $r_i$ all isomorphic to $r$, and the number $k$ is the so-called capacity of $A$. Any right-module $m$ of $A$ is a direct sum of (perhaps infinitely many) minimal submodules isomorphic to $r$. By the $A$-(right-) rank $[m:A]$, of $m$ we mean the number of minimal components in such a decomposition (i.e., the $A$-length of $m$) divided by the capacity $k$. For a left-module $m$ we introduce its left-rank $[m:A]_l$ in a similar fashion. If $m$ is a two-sided module and if it happens that $[m:A]_r = [m:A]_l$, then we shall denote the common value by $[m:A]$.

Consider a simple subring $C$ of our simple ring $A$. Let $C_r$ be the right-multiplication ring of $C$ upon $A$, and $V(C_r)$ be its commutator in the absolute endomorphism ring $\mathfrak{A}$ of $A$ as module. $V(C_r)$ is thus nothing but the $C_r$-endomorphism ring of $A$. We have $V(C_r)(V(C_r)) = C_r$. Further, $V(C_r)$ naturally contains the left-multiplication ring $A_l$ of $A$ (on $A$), since $A_l$ is the commutator in $\mathfrak{A}$ of the right-multiplication ring $A_r$, and clearly $A_r \supseteq C_r$. And $[V(C_r):A_l] = [V(C_r):V(A_l)] = [A:C]_r$. Now, if $V(C_r)$ is generated over $A_l$ by a certain number of $A_l$-semilinear endomorphisms of $A$, then we say that $C$ is weakly normal in $A$. (The notion was defined in [6; 14] in a little different way, referring to $r$, but the two definitions are equivalent, as we saw in [15].) For a nonzero $A_l$-semilinear endomorphism $\gamma$ of $A$ the submodule $\gamma A_l (= A \gamma A_l)$ of $\mathfrak{A}$ is a minimal $A_l$-two-sided module. The product of two $A_l$-semilinear endomorphisms of $A$ is naturally again an $A_l$-semilinear endomorphism of $A$. Thus our $V(C_r)$ is, when $C$ is weakly normal, a direct sum $\sum^\circ \gamma A_l$ with a certain family $\{\gamma\}$ of $A_l$-semilinear endomorphisms $\gamma$ of $A$. Another remark is that if here $C$ is strongly normal in $A$ in the sense that $V(C_r)$ is generated over $A_l$ by $A_l$-semilinear module-automorphisms of $A$, then $V(C_r)$ is generated over $A_l$ by ring-automorphisms of $A$ (which are naturally $A_l$-semilinear). For, if $\gamma$ is an $A_l$-semilinear endomorphism of $A$ and $\theta$ is the associated (ring-) automorphism of $A_l$, then $(xy)^\gamma = y^x \theta^y$ ($x, y \in A$), $x_1$ denoting the left-multiplication of $x$; or, if we consider $\theta$ also as an automorphism of $A$, then $(xy)^\gamma = x^y \gamma$. In particular $x^\gamma = x^y \gamma$. Suppose here that $\gamma$ is a (module-) automorphism. Then $1^\gamma$ must be a regular element of $A$, since $x^\gamma = x \gamma^\gamma$ vanishes for no $x \neq 0$ (i.e., for no $x^y \neq 0$) (or, since $x^\gamma 1^\gamma = 1$ for some $x$ such that $x^\gamma = 1$). Thus $(1^\gamma)^{-1} x^\gamma = (1^\gamma)^{-1} x \gamma^\gamma$, and $\gamma (1^\gamma)^{-1}$ is the product

\footnote{(4) Provided that we do not distinguish between two infinite ranks.}
of $\theta$ and the inner automorphism of $A$ induced by the regular element $1y$. So $\gamma_1=\gamma((1y)^{-1}$ is a ring-automorphism of $A$ and $\gamma_1A_1=\gamma A_1$. Taking $\gamma_1$ for each $\gamma$, we have $V_{A}(C_\gamma)=\sum \gamma_1A_1$, which proves the remark. Furthermore, the relation $C_\gamma=V_{A}(V_{A}(C_\gamma))=V_{A}(\sum \gamma_1A_1)$ shows that $C$ is the invariant system of the group generated by these (ring-) automorphisms $\gamma_1$ of $A$.

Although our main concern in our Galois theory will be the strongly normal case, the general weakly normal case is in a sense more natural and we shall continue in this section dealing with general weakly normal subrings. Now, a statement equivalent to the following lemma was proved in [14]. However, since it is rather fundamental in our theory, we shall repeat its proof very briefly in a fashion adapted to our present formulation.

**Lemma 1.1.** If $A$ is a simple ring and $C$ a weakly normal simple subring, $A$ is fully reducible as $A$-left-, $C$-right-module, that is, as $A_1C_1$-module, and is in fact a direct sum of minimal $A_1C_1$-modules which are mutually $A_1$-semilinearly and $C_1$-linearly isomorphic.

**Proof.** Let $m$ be a minimal $A_1C_1$-submodule of $A$. Let $\gamma$ be an $A_1$-semilinear endomorphism of $A$ contained in $V_{A}(C_\gamma)$. $m^\gamma$ is also an $A_1C_1$-module. In fact $u\rightarrow u^\gamma$ ($u\subseteq m$) gives an $A_1$-semilinear and $C_1$-linear mapping of $m$ onto $m^\gamma$. Since $m$ is $A_1C_1$-minimal, the same is the case for $m^\gamma$ and the mapping is an ($A_1$-semilinear and $C_1$-linear) isomorphism, unless $m^\gamma=0$. The sum of all submodules $m^\gamma$, $\gamma$ running over all $A_1$-semilinear endomorphisms of $A$ in $V_{A}(C_\gamma)$ (or, over our family $\{\gamma\}$ only), is a (nonzero) $V_{A}(C_\gamma)C_\gamma$-module. On the other hand, $A$ is homogeneously fully reducible with respect to $C_\gamma$, in the sense that it is a direct sum of mutually isomorphic minimal $C_\gamma$-modules. It follows (cf. [14]) that $A$ is $V_{A}(C_\gamma)C_\gamma$-minimal. Thus our sum $\sum m^\gamma$ coincides with $A$, which proves the lemma.

Consider a second simple subring $B$ of $A$ which contains $C$: $A\supseteq B\supseteq C$. We have:

**Lemma 1.2.** $B$ is weakly normal in $A$ together with $C$.

**Proof.** $V_{A}(B_\gamma)$ is an $A_1$-two-sided submodule of $V_{A}(C_\gamma)=\sum \gamma A_1$, and is thus, by the general theory of fully reducible modules, a direct sum of submodules ($A_1$-two-sided) isomorphic to some of $\gamma A_1$. Such a submodule has a form $\delta A_1$, with an $A_1$-semilinear endomorphism $\delta$ of $A$.

**Lemma 1.3.** Let $A$, $C$ be as in Lemma 1.1, and, as in Lemma 1.2, let $B$ be a second (necessarily weakly normal) simple subring of $A$ which contains $C$. Let $\beta$ be an isomorphism of $B$ into $A$ over $C$ (i.e., leaving $C$ elementwise fixed). Suppose that the commutator rings $V_{A}(B)$, $V_{A}(B_\beta)$ of $B$, $B_\beta$ in $A$ are simple. Then $\beta$ can be extended to an automorphism of $A$.

**Proof** (cf. [14]). $B_\beta$ is also a simple subring of $A$ containing $C$, and it is, therefore, weakly normal in $A$ too. Applying Lemma 1.1 to $B$ and $B_\beta$, in
where the $n_p$ are mutually $A$-semilinearly and $B$-linearly isomorphic minimal $A$-$B$-modules and the $\bar{n}_q$ are mutually $A$-semilinearly and $B^\theta$-linearly isomorphic minimal $A$-$B^\theta$-modules.

On the other hand, since $B$ and $B^\theta$ are isomorphic simple rings, minimal $B$-right (i.e., $B$-right-) submodules of $A$ are $(B-B^\theta, \beta)$-semilinearly isomorphic to minimal $B^\theta$-submodules of $A$; in fact, the same is the case with any minimal $B$-right- and $B^\theta$-right-modules. Hence there exists certainly a non-zero $(B-B^\theta, \beta)$-semilinear endomorphism of $A$. Let $\mathfrak{M}$ be the totality of elements in $\mathfrak{M}$ which are $(B-B^\theta, \beta)$-semilinear endomorphisms of $A$. Thus $\mathfrak{M} \neq 0$. It is contained in $V_\mathfrak{M}(C_r)$, as $\beta$ is the identity on $C$. $\mathfrak{M}$ is, further, $A$-two-sided allowable. Thus $\mathfrak{M}$ is an $A_1$-two-sided submodule of $V_\mathfrak{M}(C_r)$, and as such is a direct sum $\sum \mu A_\mu$, where the $\mu$ are $A_1$-semilinear. Thus each $\mu$ is $A$-semilinear and $(B_\ell-B^\ell, \beta)$-semilinear. There exists, hence, at least one non-zero $A_1$-semilinear and $(B_\ell-B^\ell, \beta)$-semilinear endomorphism of $A$. It follows, by the theorem of composition series, that one of the $n_p$ is $A$-semilinearly and $(B_\ell-B^\ell, \beta)$-semilinear. Then any of $n_p$ is isomorphic to any of $\bar{n}_q$ in the same sense (with, perhaps, a different automorphism of $A_1$). It follows then in particular that $n=\bar{n}$ in (1).

$V_A(B)_\ell = V_{A_1}(B_\ell)$ is the $A_1$-$B_\ell$-endomorphism ring of $A$. Since $A$ is fully reducible with respect to $A_1B_\ell$ (and the length $n$ is finite), $V_A(B)$ is a semisimple ring (with minimum condition). The same is the case with $V_A(B^\theta)$. Now we use, for the first time, our assumption that $V_A(B)$, $V_A(B^\theta)$ are simple. Then $V_A(B)_\ell$, $V_A(B^\theta)_\ell$ are simple, which implies that $n_1$, $n_2$, $\cdots$, $n_n$ are mutually $A_1B_\ell$-isomorphic (not only semilinearly but properly) and $\bar{n}_1$, $\bar{n}_2$, $\cdots$, $\bar{n}_n$ are mutually $A_1B^\ell$-isomorphic. On extending an $A_1$-semilinear and $(B_\ell-B^\ell, \beta)$-semilinear isomorphism of $n_i$ and $\bar{n}_i$, say, we may readily obtain an $A_1$-semilinear and $(B_\ell-B^\ell, \beta)$-semilinear module-automorphism of $A$, say $\mu$. It induces a ring-automorphism $\alpha$ of $A$ according to the relation $w^a = (ua)^{a_1}$ ($u, a \in A$) (i.e., $a_1^\theta = \mu^{-1}a\mu$); observe that $A_1 = V_\mathfrak{M}(A_1)$. This $\alpha$ is an extension of $\beta$, and the lemma is thus proved.

**Remark.** When $B$ is a weakly normal simple subring of a simple ring $A$, $V_A(B)$ is automatically semisimple as the endomorphism ring of a fully reducible module, as was observed in our proof. Hence, we need, in Lemma 1.3, simply to assume that $V_A(B)$ is directly indecomposable, or merely simple modulo radical, and similarly for $V_A(B^\theta)$; then they are automatically simple.

Also in connection with Lemma 1.3, we have:

**Lemma 1.4.** Let $B$ be a weakly normal simple subring of a simple ring $A$ and let the commutator $V_A(B)$ in $A$ be simple (or merely simple modulo radical);
then $B$ is strongly normal and the $B_r$-endomorphism ring $V_{A_r}(B_r)$ of $A$ is generated over $A_1$ by (ring-) automorphisms of $A$, and $B$ is the invariant system, in $A$, of the group generated by those automorphisms of $A$.

**Proof.** The $A_1B_r$-module $A$ is homogeneously fully reducible. Let $\gamma$ be an arbitrary nonzero $A_1$-semilinear endomorphism of $A$ contained in $V_{A_r}(B_r)$ and let $\theta$ be the associated automorphism of $A_1$. Consider a minimal $A_1B_r$-submodule $m$ of $A$ such that $m^\gamma \neq 0$. Then $\gamma$ gives, as in Lemma 1.1, an $A_1$-semilinear and $B_r$-linear isomorphism of $m$ and $m^\gamma$, with $\theta$ as its associated automorphism of $A_1$. Since $A$ is homogeneously fully reducible with respect to $A_1B_r$, we may extend this isomorphism to an $A_1$-semilinear and $B_r$-linear module-automorphism of $A$, say $v$, associated with the automorphism $\theta$ of $A_1$ and $v^{-1}$ are in $V_{A_r}(B_r)$, since they are $B_r$-linear. Thus $v^{-1}\gamma$ is in $V_{A_r}(B_r)$ and it is $A_1$-linear (and $B_r$-linear). Thus $v^{-1}\gamma \in V_{A_r}(B_r) \cap A_r = V_A(B_r)$, and $\gamma \in vV_A(B_r)$. Since $V_A(B)$ is a simple ring, it is generated by its regular elements. For a regular element $a$ in $V_A(B)$, $\alpha a$ is naturally an $(A_1$-semilinear) module-automorphism of $A$. Since this is the case with every $A_1$-semilinear endomorphism $\gamma$ in $V_{A_r}(B_r)$, it follows that $V_{A_r}(B_r)$ (= $\sum\gamma A_1$) has an $A_1$-basis consisting of $A_1$-semilinear module-automorphisms of $A$. Now our lemma follows from our remark concerning strongly normal subrings.

We have further:

**Lemma 1.5.** Let $A$, $C$ be as in Lemma 1.1, and let $V_{A_r}(C_r) = \sum\gamma A_1$ with $A_1$-semilinear $\gamma$. Let $\alpha$ be an automorphism of $A$ over $C$. Then $\alpha$ belongs to the same automorphism-class in $A$ as the automorphism associated with one of $\gamma$, considered as an automorphism of $A$ rather than of $A_1$.

**Proof.** Since $\alpha$ leaves $C$ elementwise fixed, $\alpha \in V_{A_r}(C_r)$ and $\alpha A_1 \subseteq V_{A_r}(C_r)$. So $\alpha A_1$ (= $A_1\alpha$) is a minimal $A_1$-two-sided submodule of $V_{A_r}(C_r)$. As such, it is ($A_1$-two-sided) isomorphic to an $A_1$. If $\theta$ is the automorphism of $A_1$ associated with $\gamma$, and if we consider it as an automorphism of $A$, then $\alpha$ belongs to the same automorphism-class in $A$ as $\theta$. Or, what amounts to the same, if we consider $\alpha$ as an automorphism of $A_1$, then it belongs to the same automorphism-class, in $A_1$, as the automorphism $\theta$ of $A_1$. For, if $\alpha$ corresponds to $\gamma a_1$ ($a \in A$) in an isomorphism of $\alpha A_1$ and $\gamma A_1$, then $a$ is regular, since $\alpha A_1 = A_1\alpha$ is mapped onto $\gamma A_1 = A_1\gamma$ whence\(^6\) $a\alpha a_1 = A_1$, $A_1 a_1^{-1} = A_1$, i.e., $A_1 a_1 = A_1$, and $x a_1 = x\alpha a_1$ corresponds to $x \gamma a_1 = x\alpha a_1 = \gamma x a_1^{-1} x\alpha a_1$ as well as to $\gamma x a_1$, whence $x a_1 = a_1^{-1} x_1 a_1$ ($x \in A$).

The following special case is well known (cf. [1]):

**Corollary.** Let $A$ be a simple ring and $Z$ be its center. If $T$ is a simple subring of $A$ containing $Z$ and finite over $Z$, then every automorphism of $A$ leaving the commutator $C = V_A(T)$ of $T$ in $A$ elementwise fixed is an inner automorphism.

\(^6\) Naturally either one of $a\alpha a_1 = A_1$, $A_1 a_1 = A_1$ is enough.
For, \( C_r = V_{\alpha}(T_r) = V_{\beta}(T_rA_1) \). \( T_rA_1 \) is a simple ring; observe that the direct product \( T_r \times A_1 \) over \( Z_r = Z_1 \) is simple and \( T_rA_1 \) is homomorphic, whence isomorphic, to it. It follows that \( V_{\beta}(C_r) = T_rA_1 \). Here the elements of \( T_r \) are \( A_1 \)-linear endomorphisms of \( A \), that is, \( A_1 \)-semilinear endomorphisms of \( A \) associated with the identity automorphism. Now the corollary follows from our lemma.

2. Regular groups of automorphisms. Let \( A \) be a simple ring. With a group \( \Phi \) of (ring-) automorphisms of \( A \), denote by \( T_\Phi \) the ring generated by all regular elements in \( A \) which effect inner automorphisms of \( A \) contained in \( \Phi \). We introduce the following:

**Definition.** A group \( \Phi \) of automorphisms of \( A \) is called complete if \( \Phi \) contains all inner automorphisms of \( A \) induced by the regular elements of \( T_\Phi \).

With any group \( \Phi \) of automorphisms of \( A \), which is not necessarily complete, the group generated by \( \Phi \) and the totality of inner automorphisms of \( A \) induced by the regular elements of \( T_\Phi \) is a complete group and is in fact the smallest complete group containing \( \Phi \). The totality of automorphisms of \( A \) leaving a certain subset of \( A \) elementwise fixed forms always a complete group. Further, if \( U \) is any subring of \( A \) containing \( T_\Phi \), the group generated by \( \Phi \) and all inner automorphisms induced by \( U \) is complete.

**Definition.** If \( \Phi \) is complete, if the ring \( T_\Phi \) is a simple ring finite over the center \( Z \) of \( A \), and if, moreover, the (invariant) subgroup \( \Phi_0 \) of \( \Phi \) consisting of all inner automorphisms of \( A \) contained in \( \Phi \) (which is also the totality of inner automorphisms of \( A \) induced by the regular elements of \( T_\Phi \) since \( \Phi \) is assumed to be complete) has a finite index \( [\Phi:\Phi_0] \) in \( \Phi \), then we say that \( \Phi \) is a regular group of automorphisms of \( A \) and \( (\Phi:\Phi_0)[T_\Phi:Z] \) is its reduced order.

Regular groups are the class of groups of automorphisms with which we want to develop our Galois theory. Needless to say, if \( A \) is in particular a field, then the requirement that \( T_\Phi \) be a simple ring is automatically satisfied and our condition amounts to the completeness plus the finiteness of \( (\Phi:\Phi_0)[T_\Phi:Z] \).

We begin with the following lemma.

**Lemma 2.1.** Let \( \Phi \) be regular. The ring \( \Phi A_1 \) \((=A_1 \Phi)\)\(^{(\ast)} \) generated by \( \Phi \) and the left-multiplication ring \( A_1 \) (in \( A \)) is a simple ring.

**Proof** (cf. [12; 13]). Let \( \Phi_0 \) and \( T_\Phi \) be as above, and denote \( T_\Phi \) simply by \( T \). Then \( \Phi_0 A_1 = T_rA_1 \), and this is a simple ring (isomorphic to the direct product \( T_r \times A_1 \) over \( Z_r = Z_1 \)). Let \( \rho_1, \rho_2, \cdots, \rho_\sigma \) \((\sigma = [\Phi:\Phi_0])\) be a representative system of \( \Phi/\Phi_0 \). Then

\[
\Phi A_1 = \rho_1 \Phi_0 A_1 \oplus \rho_2 \Phi_0 A_1 \oplus \cdots \oplus \rho_\sigma \Phi_0 A_1 = \rho_1 T_r A_1 \oplus \rho_2 T_r A_1 \oplus \cdots \oplus \rho_\sigma T_r A_1.
\]

\(^{(\ast)} \) Here \( \Phi A_1 \) (resp. \( A_1 \Phi \)) means (not the mere product but) the product-module.
The summations are necessarily direct, because \( p_1, p_2, \ldots, p_\ell \) all belong to different automorphism-classes of \( (A \text{ and }) A_\ell \) and, therefore, the \( A_\ell \)-two-sided modules \( p_1 T_A \ell, p_2 T_A \ell, \ldots, p_\ell T_A \ell \) have no isomorphic composition residue-modules. From this last it follows also that every \( A_\ell \)-two-sided submodule of \( \Phi A_\ell \) is a (direct) sum of some submodules of \( p_i T_A \ell \). In particular, a two-sided ideal \( a \) of \( \Phi A_\ell \) has this property. If \( a \neq 0 \), then \( a \) contains a certain nonzero element in one \( p_i T_A \ell \). Observing that \( T_A \ell \) is simple, we see readily that \( a = \Phi A_\ell \). The minimum condition in \( \Phi A_\ell \) is clear; it even satisfies the \( A_\ell \)- (right-, or left-) minimum condition.

Let \( I = I(\Phi) \) be the invariant system in \( A \) of our regular automorphism group \( \Phi \), that is, the totality of elements in \( A \) left invariant by \( \Phi \). Then \( I_\ell = A_\ell \cap \mathbb{A}(\Phi) = \mathbb{A}( \Phi A_\ell ) \), where \( \mathbb{A} \) denotes, as in §1, the absolute endomorphism ring of \( A \) as module. Since \( \Phi A_\ell \) is a simple ring, as we have just seen, \( A \) is homogeneously fully reducible and of finite length with respect to \( \Phi A_\ell \) and therefore \( I_\ell \) is a simple ring, and so is \( I \). Another consequence of the simplicity of \( \Phi A_\ell \) is

\[
V\mathbb{A}(I_\ell) = \Phi A_\ell.
\]

(2) shows then that \( I \) is weakly normal in \( A \); in fact, it is strongly normal. Further, \([A : I]_\ell = [A_\ell : I_\ell]_\ell = [V\mathbb{A}(I_\ell) : \mathbb{A}(A_\ell)]_\ell = [\Phi A_\ell : A_\ell]_\ell \), and this is equal to \( g[T_A \ell : A_\ell]_\ell = g[T : Z] \).

**Theorem 1.** Let \( \Phi \) be a regular group of automorphisms of a simple ring \( A \), and \( I = I(\Phi) \) be its invariant system. Then \( I \) is a simple ring and \( A \) has an independent right- (resp. left-) basis over \( I \) consisting of as many terms as the reduced order \( (\Phi : \Phi_0)[T_\Phi : Z] \) of \( \Phi \). \( \Phi \) exhausts the automorphisms of \( A \) elementwise fixed. The commutator \( V_A(I) \) of \( I \) in \( A \) coincides with \( T = T_\Phi \).

**Proof.** The first half has been seen; observe that \([A : I]_\ell = g[T : Z] \), too, by symmetry. To prove the second half, let \( \alpha \) be an automorphism of \( A \) over \( I \). By Lemma 1.5, together with (3) and (2), we see that \( \alpha \) has a form \( \rho_\phi \phi_0 \) (an inner automorphism of \( A \)) \( (\phi_0 \in \Phi_0) \). This inner automorphism of \( A \) must leave \( I \) elementwise fixed, since \( \alpha, \rho_\phi \), and \( \phi_0 \) do, and is then induced by an element in \( V_A(I) \). Here, as asserted in our theorem,

\[
V_A(I) = T(= T_\Phi),
\]

since \( V_A(I_\ell) = A_\ell \cap V\mathbb{A}(I_\ell) = A_\ell \cap \Phi A_\ell = T_\ell \); observe that the sum \( \sum \rho_i A_\ell A_\ell \) is, as (2), direct and that the product \( A_\ell A_\ell \) in \( \mathbb{A} \) is direct over \( Z_\ell = Z_\ell \). Thus our inner automorphism belongs to \( \Phi_0 \). Hence \( \alpha \in \rho_i \Phi_0 \), and \( \alpha \) belongs to \( \Phi \).

Now, the invariant system, in \( A \), of \( \Phi_0 \) is nothing but the commutator \( V_A(T) \) of \( T = T_\Phi \). Put \( S = V_A(T) \). As a special case of our theorem (applied to \( \Phi_0 \) instead of \( \Phi \)), and as is well known, \( S \) is a simple ring and

\[
\]
The following theorem is of particular significance in the special case $U = T$ (whence $R = S$):

**Theorem 2.** Let $\Phi$ be a regular group of automorphisms of a simple ring $A$ and $\Phi_0$ be its (invariant) subgroup of inner automorphisms. Let $U$ be a simple subring containing $T (= T_0)$ and finite over the center $Z$ of $A$. Assume that $U$ is setwise invariant under $\Phi$, that is, $U^\Phi = U$. Then $\Phi/\Phi_0$ is an outer group of automorphisms of the commutator $R = V_A(U)$. Its invariant system $I/R$ in $R$ is a simple ring, $[R : I/R] = (\Phi/\Phi_0)$, and $\Phi/\Phi_0$ exhausts the automorphisms of $R$ over $I/R$. The product-module $RI$ (resp. $IR$) is a ring and coincides indeed with $S = V_A(T)$.

**Proof.** Since $R \subseteq S$, clearly $\Phi_0$ induces on $R$ the identity automorphism. Suppose that $\phi \in \Phi$ induces an inner automorphism on $R$, induced by an element $a$ of $R$. Denote by $a$ the inner automorphism of $A$ induced by this element $a$. Then $\phi a^{-1}$ is an automorphism of $A$ leaving $R$ elementwise invariant. As such, it is an inner automorphism of $A$, by the corollary to Lemma 1.5. Then $\phi$ must be an inner automorphism of $A$ too; $\phi \in \Phi_0$. Thus $\Phi/\Phi_0$ is an outer group of automorphisms of $R$.

$\Phi/\Phi_0$ is in particular a regular automorphism group of $R$. Its invariant system in $R$ is evidently the intersection $I\cap R$ of $R$ and the invariant system $I$ in $A$ of $\Phi$. On applying Theorem 1 to $R$ and $\Phi/\Phi_0$ (instead of $A$ and $\Phi$) we see that $[R : I\cap R] = [R : I\cap R] = (\Phi/\Phi_0)$ and $\Phi/\Phi_0$ exhausts all automorphisms of $R$ leaving $I\cap R$ elementwise fixed.

Clearly $V_A(T) = S$ contains both $I$ and $R$, hence $RI$. Let $(w_1, w_2, \ldots, w_g)$ $(g = (\Phi/\Phi_0))$ be an independent right-basis of $R$ over $I\cap R$ (which exists by the outer special case of Theorem 1). Then the matrix.

$$
\begin{bmatrix}
  w_1^{\rho_1} & w_2^{\rho_1} & \cdots & w_g^{\rho_1} \\
  \vdots & \vdots & \cdots & \vdots \\
  w_1^{\rho_g} & w_2^{\rho_g} & \cdots & w_g^{\rho_g}
\end{bmatrix}
$$

is regular, where $\rho_1, \rho_2, \ldots, \rho_g$ form, as in (2), a representative system of $\Phi/\Phi_0$. For, if $(x_1, x_2, \ldots, x_g)$ is a vector in $R$ such that $(x_1, x_2, \ldots, x_g)$ $(w_i^{\rho_i}) = 0$, then $\sum x_i y_i = 0$ for every element $y$ in $R$ ($= w_1(I\cap R) \oplus w_2(I\cap R) \oplus \cdots \oplus w_g(I\cap R)$). But $\rho_1, \rho_2, \ldots, \rho_g$ are right-independent over the left-multiplication ring of $R$ (on $R$), again by the special case $A = R$ of the directness of (2). Hence necessarily $x_1 = x_2 = \cdots = x_g = 0$, which proves that our matrix is regular. Then $w_1, w_2, \ldots, w_g$ are right-independent over $I$ too. For, if $w_1 a_1 + w_2 a_2 + \cdots + w_g a_g = 0$ with $a_j \in I$, then $w_1 a_1 + w_2 a_2 + \cdots + w_g a_g = 0$ for every $i = 1, 2, \ldots, g$, that is, $(w_i^{\rho_i})(a_j) = 0$. Hence $a_1 = a_2 = \cdots = a_g = 0$ necessarily. Thus $RI = w_1 I \oplus w_2 I \oplus \cdots \oplus w_g I$ and $[R : I] = g$. But $[S : I] = g$ too, according to the special case $R = S$ of the already established part of our theorem. So $S = RI$. Similarly we have $S = IR.$
Our theorem is somewhat complicated. But it reveals how the invariant system $I$ of a regular group is situated in $A$. In particular, it shows how $I$ is related to $R$ which is (the commutator of $U$ and is) of purely inner character in $A$, while $I \cap R$ is of purely outer character in $R$. We repeat that the case $U=T$ (whence $R=S$) is of particular significance, whereas if $[A:Z]<\infty$, then we may take $A$ itself as $U$ letting thus $R$ be the center $Z$ of $A$.

In connection with our theorem we may also note that every automorphism of $R$ over $I \cap R$ is (in $\Phi$, or, more precisely, in $\Phi/\Phi_0$, and therefore, evidently) extended to an automorphism of $S=RI=IR$ over $I$, and indeed in a unique manner. Further, $[S:I]=g=[R:I \cap R]$ and

$$[S:I \cap R]=[S:I][I:I \cap R]=[R:I \cap R][I:I \cap R].$$

For, (6) is certainly true if we restrict ourselves either to right- or to left-ranks. But $I \cap R$ is the invariant system, in $A$, of the (regular) group generated by $\Phi$ and the inner automorphisms effected by $U$. Hence $[A:I \cap R]_i=[A:I \cap R]_i$, and therefore $[S:I \cap R]_i=[S:I \cap R]_i$, since $[A:S]_i=[A:S]_i$. Similarly $[I:I \cap R]_i=[I:I \cap R]_i$.

### 3. Subrings with simple commutators.

In connection with Theorem 1, as well as Lemmas 1.3 and 1.4, we are led to consider simple subrings of $A$ whose commutators, in $A$, are also simple.

**Theorem 3.** Let $B$ be a simple subring of a simple ring $A$ such that $[A:B]<\infty$. If the commutator $V_A(B)$ of $B$ in $A$ is simple, then the group $\Phi$ of all automorphisms of $A$ over $B$ is regular. If (and only if) $B$ is weakly normal in $A$, the invariant system $I$ of $\Phi$ coincides with $B$.

**Proof.** Set $T=V_A(B)$. The subgroup $\Phi_0$ of all inner automorphisms of $A$ contained in $\Phi$ is clearly the totality of inner automorphisms induced by the regular elements of $T$, and thus $T=T_\Phi$. Here $T$ is simple, by assumption. Moreover, $[T:Z]=[T:A_1:A_1]$, since the product $A_1A_1$ is direct over $Z_1=Z_1$. Here $T_1A_1 \subseteq V(B_t)$, and $[V(B_t):A_1]=[V(B_t):V(A_t)]=A_t:B_t]$, $[A:B]<\infty$. Thus $[T:Z]<\infty$. Further, if $\rho_1, \rho_2, \ldots$ are representatives of $\Phi/\Phi_0$, then they all belong to different automorphism-classes and thus are right-independent over $A_t$, by the argument used in proving the directness of (2). The relation $[V(B_t):A_1]<\infty$ shows then also that $(\Phi/\Phi_0)<\infty$. Thus $\Phi$ is regular.

The second half of the theorem, which is in fact far deeper than the first half, follows from Lemma 1.4 (the "only if" part being clear from Theorem 1).

Given a regular group $\Phi$ of automorphisms, Theorems 1 and 3 suffice to establish 1-1 Galois correspondence between regular subgroups of $\Phi$ and simple subrings, containing the invariant system $I$ of $\Phi$, with simple commutators. However, postponing the statement until the next section, we consider the case where a subring $B$ is not known to contain the invariant system of a regular group and is not known to be weakly normal.
Theorem 4. Let \( B \) be a simple subring of a simple ring \( A \) such that \([A:B] < \infty\) and the commutator \( T = V_A(B) \) is simple. Let \( \Phi \) be the group of automorphisms of \( A \) over \( B \), and let \( U \) be a simple subring of \( A \) containing \( T \) and finite over the center \( Z \) of \( A \) (or, what is the same, \([U:T] < \infty\)) such that \( U^\Phi = U \), and put \( R = V_A(U) \). Let \( W \) be the invariant system in \( R \) of \( \Phi \). Then the ring generated by \( W \) and \( B \) coincides with the invariant system of \( \Phi \) in \( A \).

(Observe that \( \Phi \) induces an outer automorphism group on \( R \) as in Theorem 2, and thus our theorem reduces, in a sense, the problem of the invariant system to purely outer and purely inner situations. Again the case \( U = T \) (whence \( R = S (= V_A(T)) \)) is of importance.)

Proof. The group \( \Phi_1 \) generated by \( \Phi \) and the totality of inner automorphisms of \( A \) induced by the regular elements of \( U \) is a regular automorphism group. Its invariant system in \( A \) is nothing but \( W \). Now, let \( Q \) be the subring of \( A \) generated by \( B \) and \( W \). Since \( B, W \subseteq V_A(T) \), we have \( Q \subseteq V_A(T) \) and \( V_A(Q) \subseteq T \). On the other hand, \( V_A(Q) \subseteq V_A(B) = T \). Hence \( V_A(Q) = T \) and this is simple. As \( Q \supseteq W \) and \( W \) is weakly (in fact, strongly) normal in \( A \), \( Q \) is weakly normal in \( A \), because of Lemma 1.2. By Theorem 3, \( Q \) is then the invariant system of a certain regular automorphism group of \( A \). This group is, however, clearly our \( \Phi \), and the theorem is proved.

4. Galois theory.

Theorem 5. Let \( \Phi \) be a regular automorphism group of a simple ring \( A \), and \( I = I(\Phi) \) be its invariant system. Then there is a 1-1 dual correspondence between regular subgroups of \( \Phi \) and simple subrings of \( A \) containing \( I \) and possessing simple \(^{(1)}\) commutators in \( A \), in the usual sense of Galois theory.

Proof. Theorems 1, 3, applied to subgroups and subrings, give the desired Galois correspondence.

Theorem 6. Let \( A, \Phi, I \) be as in Theorem 5. If \( B, B^\Phi \) are two (not necessarily distinct) simple subrings of \( A \) containing \( I \) and possessing simple commutators, and if there exists an isomorphism \( \beta \) of \( B \) and \( B^\Phi \) leaving \( I \) element-wise fixed, then the isomorphism \( \beta \) can be extended to an automorphism of \( A \) which is necessarily contained in \( \Phi \).

Proof. Immediate from Lemma 1.3.

Thus we have been able to establish for \( A, \Phi \) the two main features in Galois theory, i.e., the Galois correspondence and the extension of isomorphisms over the invariant system. Next consider a simple subring \( B \) of \( A \), with simple commutator, containing \( I = I(\Phi) \) and consider the subgroup \( \Psi \) of \( \Phi \) corresponding to \( B \) in the sense of Galois correspondence; thus \( \Psi \) is the group of all automorphisms (necessarily contained in \( \Phi \)) of \( A \) over \( B \). Then \( \Psi \) is a normal subgroup of \( \Phi \) if and only if \( B^\Phi = B \). The invariant sys-

\(^{(1)}\) Or, simple modulo radical. Cf. §1 or §4, (ii).
tem in $B$ of the automorphism group $\Phi/\Psi$ of $B$ is then exactly $I$. However, we are interested in a little more general situation and want to obtain a condition in order that $I$ be the invariant system in $B$ of $\Lambda/\Psi$, where $\Lambda$ is the totality of elements of $\Phi$ which leave $B$ setwise invariant\(^{(8)}\). We begin with the following lemma.

**Lemma 4.1.** Let $A$, $\Phi$, $I$ be as in Theorem 5. Let $B$ be a simple subring of $A$ containing $I$ and possessing a simple commutator $D = V_A(B)$. Let $\Lambda$ be the totality of elements of $\Phi$ which map $B$ into itself\(^{(9)}\), and let $V$ be the ring generated by all the regular elements of $A$ which induce inner automorphisms of $A$ belonging to $\Lambda$\(^{(10)}\). If $V_T(D) = T \cap V_A(D)$ is contained in $V$\(^{(11)}\), and if the product, in $A$, of the centers $Y$, $Z_T$ of $D$ and $T$ is semisimple, then $V$ is semisimple too.

**Proof.** Put $\Lambda_0 = \Lambda \cap \Phi_0$. $V$ is nothing but the subring of $A$ generated by the regular elements inducing the elements of $\Lambda_0$. Now $\Lambda_0$ leaves $B$, hence $D = V_A(B)$, setwise fixed. Let $\Gamma$ be the totality of elements of $\Lambda_0$ which induce on $D$ inner automorphisms of $D$. Thus $\Gamma$ is nothing but the totality of elements of $\Lambda_0$ leaving the center $Y$ of $D$ elementwise fixed; observe that, since $[D:Y] \leq [D:Z] \leq [T:Z] < \infty$, every automorphism of $D$ leaving $Y$ elementwise fixed is inner. Thus $\Lambda_0/\Gamma$ is an automorphism group of $Y$. It leaves $Z$ elementwise fixed. Since $[Y:Z] \leq [D:Z] < \infty$, $(\Lambda_0/\Gamma)$ is finite. Let $\beta_1, \beta_2, \ldots, \beta_m$ be a representative system of $\Lambda_0/\Gamma$, and $b_1, b_2, \ldots, b_m$ be the regular elements of $\Gamma$ inducing $\beta_1, \beta_2, \ldots, \beta_m$. Since for each pair $i, j$ we have $b_i b_j = b_k V_D(D)$ with some $k$,

\begin{equation}
\sum b_i V_T(D)D + b_2 V_T(D)D + \cdots + b_m V_T(D)D
\end{equation}

is a ring. In fact, it coincides with ring $V$ because of our assumption $V_T(D) \subseteq V$. Since $\beta_1, \beta_2, \ldots, \beta_m$ induce automorphisms of $D$ all in different automorphism-classes, the minimal $D$-two-sided modules $b_1 D, b_2 D, \ldots, b_m D$ are all nonisomorphic. Hence no two of $b_1 V_T(D)D, b_2 V_T(D)D, \ldots, b_m V_T(D)D$ have isomorphic composition residue-modules. Thus the sum (7) must be direct and, moreover, any $D$-two-sided submodule of the sum, i.e., $V$, is a sum of submodules of the summands. In particular this last is the case for any two-sided ideal of $V$. It follows readily that if $N$ is the radical of $V_T(D)D$, then $b_1 N \oplus b_2 N \oplus \cdots \oplus b_m N$ is the radical of $V$; by the way, $V_T(D)D (\subseteq T)$ and $V$ are finite algebras over $Z$, say. Here $V_T(D) = V_T(Z_T D)$ and $V_T(D)D = V_T(Z_T D)Z_T D$. Since $Y \subseteq T$, $Z_T Y$ is commutative (and finite over $Z$). Suppose now, as was stated in the lemma, that $Z_T Y$ is semisimple (hence is a direct sum of a finite number of mutually

\(^{(8)}\) In other words, $\Lambda$ is the normalizer of $\Phi$ in $\Phi$.

\(^{(9)}\) Then they map $B$ onto itself isomorphically; observe that $[A:B] < \infty$.

\(^{(10)}\) Thus $V$ is nothing but $T_A$.

\(^{(11)}\) Instead of assuming this, we may assume that $(V \cap V_T(D)) D$ is semisimple, as our proof will show.

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
orthogonal fields). Then $Z_TD$ is a semisimple algebra over $Z$, say; it is in fact the direct product $Z_T Y \times D$ over $Y$. Then $V_T(Z_TD)$ is also a semisimple algebra and so is $V_T(Z_TD)Z_TD$, too, $Z_T Y$ being their common center (cf. [17] e.g.). Hence $N=0$ and $V$ is semisimple, as was observed above, which proves the lemma.

Now we have:

**Theorem 7.** Let $A, \Phi, I$ be as in Theorem 5. Let $B$ be a simple subring of $A$ containing $I$ and possessing a simple commutator in $A$. Let $\Lambda$ be the totality of elements of $\Phi$ which map $B$ into itself. Assume that $T_\Lambda$ contains $T_\Phi \cap V_A(V_A(B))$ (12). In order that the invariant system of $\Lambda$ in $B$ coincide with $I$ it is necessary and sufficient that $\Phi$ be the smallest complete group of automorphisms of $A$ containing $\Lambda$.

**Proof.** Suppose that the last condition is satisfied. Then the invariant system of $\Lambda$ in $A$ coincides with that of $\Phi$, that is, $I$. Furthermore, the invariant system of $\Lambda$ in $B$ is $I$.

Suppose conversely that the invariant system of $\Lambda$ in $B$ coincides with $I$. Then the invariant system of $\Lambda$ in the center $Y$ of the (simple) commutator $D = V_A(B)$ of $B$ is clearly $I \cap Y$. On the other hand, $Y \subseteq D = V_A(B) \subseteq V_A(I)$. Hence $I \cap Y$ is contained in the center $Z_I = I \cap V_A(I)$ of $I$. Thus $Z_I \cap Y$ contains, hence coincides with the invariant system $I \cap Y$ of $\Lambda$ in $Y$. Therefore $Y$ is (finite and) separable over $Z_I \cap Y$; for the finiteness observe that $(Z : I \cap Z)\le (\Phi : \Phi_0) < \infty$, $(Y : Z) < \infty$.

On the other hand, $Z_T \cap Y = V_A(T) \cap T \cap Y = V_A(T) \cap Y = S \cap Y \supseteq I \cap Y \supseteq Z_I \cap Y$, where $Z_T$ denotes, as in Lemma 4.1, the center of $T = T_\Phi$ and $S$ is $V_A(T)$. Hence $Y$ is (finite and) separable over $Z_T \cap Y$ too. Then the direct product $Z_T \times Y$ over $Z_T \cap Y$ is semisimple, and so is the product $Z_T Y$ in $A$. Hence, if we denote $T_\Lambda$ by $V$, as in Lemma 4.1, then $V$ is semisimple, by the same lemma.

Thus, the smallest complete group containing $\Lambda$ has the following property which is very close to regularity: it is complete, its subgroup of inner automorphisms has a finite index, and the ring $V$, generated by the regular elements inducing the inner automorphisms in it, is semisimple (and finite over $Z$, naturally), instead of being simple. However, as we shall observe in the next section, the last two statements in Theorem 1, in particular, are valid also for such a group. Now, on the other hand, the invariant system of $\Lambda$ in $A$ is $I$; observe that $\Lambda$ contains all automorphisms of $A$ over $B$ and there-

(12) This condition is very awkward, but it is automatically satisfied in case $A$ is finite over $Z$; see §5, iv. Further, the sufficiency assertion in our theorem is independent of this assumption.

This assumption may be replaced by the requirement that $(T_\Lambda \cap V_A(V_A(B))V_A(B)$ be semisimple, which is automatically the case certainly when $A$ (or $T_\Phi$) is a sfield; cf. footnote 11.

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
fore the invariant system of $A$ in $\mathcal{A}$ is in any event contained in $B$. Our smallest complete group containing $A$ has also the invariant system $I$ in $A$. On assuming the above mentioned (as yet unverified) generalization of the exhaustion statement of Theorem 1, we see then that it is the totality of automorphisms of $A$ over $I$ and is thus nothing but $\Phi$, which proves the theorem.

Remark. Since the completion of $A$ turns out to be identical with $\Phi$ and therefore regular, the ring $V = T_A$ is, in case of Theorem 7, nothing but $T = T_\Phi$ and, in particular, simple. The "reason" for this is that, in the notations of the proof of Lemma 4.1, $\Lambda_0$ is big enough so that a simple component in the semisimple ring $V_T(D)D$ is carried to any other simple component by one of $\beta_1, \beta_2, \cdots, \beta_m$, making thus (7), which is $V$, simple (in spite of the fact that $V_T(D)D$ may not be simple). Observe also that we did not assume the semisimplicity of $V_T(D)D$ (nor of $Z_T Y$), but proved it.

5. Supplementary remarks. (i) Semi-regular groups. In our proof of Theorem 7 we were led to consider a generalization of regularity for automorphism groups. Thus we want to call an automorphism group $\Phi$ of a simple ring $A$ semi-regular if $\Phi$ is complete, $(\Phi : \Phi_0) < \infty$, and if the ring $T_\Phi$ is semisimple and finite over $Z$, the center of $A$. In fact, some of our results concerning regular groups remain valid for semi-regular groups. Let, namely, $\Phi$ be semi-regular, and consider $\Phi A_I$. A modification of our proof of Lemma 2.1 shows that $\Phi A_I$ is a semisimple ring, with minimum condition; consider either the radicals of $T = T_\Phi$ and $\Phi A_I$ or the lattices of two-sided ideals in $T$ and $\Phi A_I$. The invariant system $I = I(\Phi)$ of $\Phi$ is then a semisimple ring, with minimum condition, too, and (3) and (4) remain valid. If we define, as we in fact did in [14], the weak normality for arbitrary, not necessarily simple, subrings of $A$ in exactly the same manner as we did for simple rings, in §1, then Lemma 1.5 is true for any such arbitrary weakly normal subring $C$ of $A$. (Its corollary is the case for any semisimple (or, more generally, uni-serial, for instance) subring $T$ finite over $Z$.) Taking this into account, we see readily that $\Phi$, a semi-regular automorphism group of $A$, exhausts the automorphisms of $A$ over $I = I(\Phi)$. The last statement of Theorem 1 remains true too. It is also possible to obtain some statements which may be considered as a generalization of our rank relation, but they are rather complicated and clumsy. (An exact transfer of the rank relation can be made if the $T_A$-submodules of $A$ corresponding to different simple subrings of (semisimple) $T_A$ all have equal ranks with regard to respective simple subrings of $T_A$ ($T = T_\Phi$), and this is in fact the case which has been considered in [13] under a general setting that $A$ be $T_A$-"regular.") Also the first statement of Theorem 2 is true for a semi-regular group $\Phi$, and in fact for a semisimple $U$. In dealing with semi-regular automorphism groups, we have naturally to consider not only simple, but semisimple subrings of $A$, so the present supplementary remark (i) is closely related to the latter part of the succeeding remark (ii).

(ii) The condition of simple commutators. We considered, in our Galois
theory, those subrings of $A$ whose commutators in $A$ are simple. In general, there are simple subrings of $A$ containing the invariant system $I$ of a regular group $\Phi$ whose commutators are not simple and which in fact are not invariant systems of automorphism groups; see [18] or [7, p. 298]. We note however that if in particular $\Phi_0 = \Phi$ or $=1$, i.e., if $\Phi$ is either an inner or an outer automorphism group, then the condition is satisfied automatically, that is, every simple subring of $A$ containing $I$ has a simple commutator and is the invariant system of the corresponding subgroup of $\Phi$.

As we observed in a remark in connection with Lemma 1.3, a superfluous weakening of the requirement can be made by demanding that the commutator be simple modulo radical. In regard to (Lemma 1.3 and) Theorem 6, it is also possible to weaken the condition somewhat in a more essential manner by assuming, for instance, that the commutator is semisimple and the capacities of its simple components are all equal, together with some further requirements in connection with $\Phi$. However, the condition is needed more definitely in regard to (Lemma 1.4 and) the Galois correspondence; cf. the example of Teichmüller alluded to above.

(iii) The condition of simple commutators (continued). It might be of some interest and use to observe that instead of demanding directly the simpleness of the commutator $V_A(B)$ of $B$, where $B$ is a subring of $A$ containing the invariant system $I = I(\Phi)$ of a regular automorphism group $\Phi$, we may demand that the commutator $V_A(RB)$ of the product (or, of the ring generated by $R$, $B$) be simple, where $R$ is any subring of $S = V_A(T_\Phi)$. For, since $V_A(R) \supseteq V_A(S) = T_\Phi = V_A(I) \supseteq V_A(B)$, we have $V_A(RB) = V_A(B)$.

(iv) Algebra case. In the case where our simple ring $A$ is finite over its center $Z$, every automorphism of $A$ leaving $Z$ elementwise fixed is inner, and the Galois theory of $A$ is, roughly speaking, a combination of the theory of inner automorphisms of $A$ and the Galois theory of the (commutative) field $Z$ (see Hochschild [7]; cf. also Baer [4]). In fact, our $U$ in Theorem 2 may be chosen to be $A$ itself (in case $[A:Z] < \infty$), giving $R = Z$. Thus the theorem and a remark which accompanied it, at the end of §2, show that if $I$ is the invariant system of a regular automorphism group, $ZI$ is simple, $[Z:Z \cap I]$ is finite, and the product $ZI$ is direct over $Z \cap I$, showing that $I$ is regular in the sense of [7, Definition 2.3]. So, our Theorems 1, 2, together with the accompanying remark, generalize [7, Theorem 2.1]. On the other hand, (if $[A:Z] < \infty$ and) if $ZB$ is simple, then the commutator $V_A(B)$ is simple too. Thus an almost regular subring $B$ in the sense of [7, Definition 2.3] is nothing but a simple subring with simple commutator, and our Theorems 3, 4 form a generalization of [7, Theorem 2.2]. (We could also apply our above remark (iii) to $R = Z$.) Needless to say, our Theorem 6 specializes to [7, Theorem 2.4] in case of an algebra $A$. Further, our Theorem 7 generalizes Theorem 2.5 in [7]. Indeed, our side condition $T_\Phi \cap V_A(V_A(B)) \subseteq T_A$ is automatically satisfied in case $[A:Z] < \infty$. Observe, to see this, that $V_A(V_A(B)) = ZB$ (in case
$[A:Z]<\infty)$. Taking a $B$-basis of $ZB$ consisting of elements of $Z$ and observing that $T_\Phi = V_A(I)$ ($I \subseteq B$) we see readily that $T_\Phi \cap ZB = Z(T_\Phi \cap B)$, and this last product is contained in $T_A$ since both $Z$ and $T_\Phi \cap B (= V_B(I))$ are contained in $T_A$. We note also that our Theorem 7 improves [7, Theorem 2.4] in the algebra case by showing that the assumption of the simpleness of $I \cdot (\text{center of } B) \cdot Z (= LPC \text{ in the notation of } [7])$ is rather unnecessary.

(v) **Field case.** Concerning the case of a field $A$, we merely mention the following facts. Firstly, and methodologically, $A$ is trivially minimal (hence homogeneously fully reducible) with respect to any operator domain containing $A_1$, say. Secondly, and with respect to the results formulated, every subring possesses a simple (in fact, field) commutator, and $T_\Phi$ is, again trivially, a simple ring (in fact a field) for any automorphism group $\Phi$.

(vi) **Complete primitive rings.** Our theory can easily be extended to the case of a complete primitive ring (cf. [6; 10; 11; 16]; they were called closed irreducible in [11; 16]). It is in fact possible to transfer our arguments step by step to this case. However, without doing so, let us observe that Galois theory of such a ring, with respect to a regular automorphism group (of finite reduced order), can be reduced to that of a simple ring. Let, namely, $A$ be a (right-) complete primitive ring, and $\Phi$ be a regular automorphism group of $A$, defined exactly in the same manner as in §2. Thus $T_\Phi$ is a simple ring finite over the center $Z$ of $A$. We consider

\begin{equation}
\Phi A_r = \rho_1 T_1 A_r + \rho_2 T_2 A_r + \cdots + \rho_\nu T_\nu A_r
\end{equation}

(rather than $\Phi A_1$), where $T = T_\Phi$ and $\rho_1$, $\rho_2$, $\cdots$, $\rho_\nu$ form a representative system of $\Phi/\Phi_0$. Here $T_i A_r$ ($\simeq T_i \times A$, over $Z_i = Z_r$) is a complete primitive ring too. Let $\mathfrak{g}$ be the (unique) smallest two-sided ideal of $A$. Minimal $A_r$-two-sided modules $\rho_1 \mathfrak{g}_r$, $\rho_2 \mathfrak{g}_r$, $\cdots$, $\rho_\nu \mathfrak{g}_r$ are all mutually nonisomorphic, the proof being similar to the one in [16, Lemma 7]. Hence no two of the $A_r$-two-sided modules $\rho_1 T_1 \mathfrak{g}_r$, $\rho_2 T_2 \mathfrak{g}_r$, $\cdots$, $\rho_\nu T_\nu \mathfrak{g}_r$ have mutually isomorphic composition residue-modules. A fortiori, they have no mutually isomorphic composition residue-modules as $T_i A_r$-two-sided modules. Here $T_i \mathfrak{g}_r$ is the smallest two-sided ideal of $T_i A_r$, and it follows that the automorphisms of $T_i A_r$ induced by $\rho_1$, $\rho_2$, $\cdots$, $\rho_\nu$ all belong to different automorphism-classes (of $T_i A_r$). By [16, Theorem 14] our $\Phi A_r$ is a primitive ring with minimal right- (or left-) ideals, the directness of the summation in (8) being immediate. Let $\mathfrak{n}$ be a minimal right-ideal of $\Phi A_r$, and denote by $\mathfrak{N}$ the absolute endomorphism ring of $\mathfrak{n}$. Then $\mathfrak{n}$ is a direct sum of a finite number of faithful minimal $T_i A_r$-(right-) modules, as is seen from the proof of Theorem 14 in [16]. Also, $\mathfrak{n}$ is a direct sum of a finite number of faithful minimal $A_r$-modules. Thus the $A_r$-endomorphism ring $V_\mathfrak{N}(A_r)$ of $\mathfrak{n}$ is a simple ring (with minimum condition). Further, $V_\mathfrak{N}(V_\mathfrak{N}(A_r)) = A_r$. For each $\rho \in \Phi$ we have $\rho^{-1} V_\mathfrak{N}(A_r) \rho$.
= V_{\mathfrak{R}}(A_r), \text{ since } \rho^{-1}A_r\rho = A_r, \text{ and each } \rho \text{ induces thus an automorphism of } V_{\mathfrak{R}}(A_r). \text{ By } [16, \text{ Theorem 5}] \text{ it is readily seen that } \rho_1, \rho_2, \ldots, \rho_g \text{ induce automorphisms of } V_{\mathfrak{R}}(A_r) \text{ all belonging to distinct automorphism-classes of } V_{\mathfrak{R}}(A_r). T_rV_{\mathfrak{R}}(A_r) (\cong T_r \times_{\mathfrak{s}} V_{\mathfrak{R}}(A_r)) \text{ is a simple ring and }

(9) \quad \rho_1T_rV_{\mathfrak{R}}(A_r) + \rho_2T_rV_{\mathfrak{R}}(A_r) + \cdots + \rho_gT_rV_{\mathfrak{R}}(A_r)

is also a simple ring, as we readily see, either as above or as in Lemma 2.1 (together with the directness of the sum); for the ring property of (9) observe that \( V_r(A_r) \supseteq T_1 \leq \Phi A_r \) and thus \( \Phi_0 \subseteq T, T_1 \subseteq T_rV_{\mathfrak{R}}(A_r) \). \( \pi \) is, hence, decomposed into a direct sum of (perhaps infinitely many) submodules minimal with respect to (9). Let

(10) \quad \pi = \cdots \oplus \pi_n \oplus \cdots

be such a decomposition of \( \pi \). All \( \pi_n \) are isomorphic with respect to (9), and a fortiori with respect to \( V_{\mathfrak{R}}(A_r) \). Let \( \{\epsilon_{ir}\} \) be a system of matrix unit endomorphisms of \( \pi \) with respect to this homogeneous decomposition (10). The \( \epsilon_{ir} \) are in \( A_r (= V_{\mathfrak{R}}(V_{\mathfrak{R}}(A_r))) \). They also commute with every element of (9) and thus are invariant under \( \Phi \). Then \( \epsilon_{11}A_r\epsilon_{11} \) is setwise invariant under \( \Phi \), and \( \Phi \) can be considered as its automorphism group. Now \( \epsilon_{11}A_r\epsilon_{11} \) is a simple ring (with minimum condition), since \( \pi_1 \) (and in fact every \( \pi_n \)) is a direct sum of a finite number of minimal \( V_{\mathfrak{R}}(A_r) \)-modules, and \( \Phi \) is regular as its automorphism group, as we see readily. The Galois theory of \( A \) with respect to \( \Phi \) can now be reduced to that of the simple ring \( \epsilon_{11}A_r\epsilon_{11} \), with respect to \( \Phi \); the argument is parallel with [16, §7].

(vii) Regular groups of infinite reduced orders. The first step in generalizing our theory to an automorphism group of infinite reduced order (in the natural sense) is to allow either \( (\Phi: \Phi_0) \) or \( (T_{\Phi}:Z) \) to be infinite and to restrict the other to be finite. Each case produces difficulties. With respect to the first, Jacobson has recently established an elegant infinite outer Galois theory \( (\Phi_0 = 1) \) for a field \( A \). The writer has collaborated with him in extending the theory to the case \( \Phi_0 \neq 1 \) under more restrictions than \( (T_{\Phi}:Z) < \infty \). But the last result still seems indecisive.

The writer is grateful to G. Hochschild who has suggested certain necessary revisions.

Bibliography


18. O. Teichmüller, *Über die sogenannte nichtkommutative Galoissche Theorie und die Relation $\xi_{\mu,\eta} \xi_{\lambda,\mu} = \xi_{\lambda,\eta}$*, Deutsche Mathematik vol. 5 (1940) pp. 138–149.

*University of Illinois, Urbana, Ill.*