# GALOIS THEORY OF CONTINUOUS TRANSFORMATION RINGS(1)

BY

ALEX ROSENBERG AND DANIEL ZELINSKY

1. **Introduction.** Let $A$ be a ring isomorphic to the ring $\mathcal{L}(M, N)$ of all continuous linear transformations on a pair of dual vector spaces $(M, N)$ over a division ring $D$—i.e. on a weakly topologized vector space $M$. Such a ring will be called a continuous transformation ring. (For further details on weak topologies and continuous transformation rings, see §2 and the references given there.) Important special cases are (1) when $N$ is the full dual of $M$ then $A$ is any completely primitive ring: all linear transformations on a vector space; (2) when $M$ is finite dimensional then the topology is discrete and $A$ becomes a typical simple ring with minimum condition; (3) when $M$ is one-dimensional, $A$ is a division ring (anti-isomorphic to $D$); and (4) the ring of all bounded operators on a Banach space.

Following Artin [1], the Galois theory of $A$ consists in studying the subrings $C_0$ of $A$ which are invariant rings under groups of automorphisms of $A$ (the group being finite in some sense). In particular, if $C_0$ is such a ring and $\Gamma_0$ the group of all automorphisms of $A$ over $C_0$, we develop the usual Galois correspondence between certain subgroups of $\Gamma_0$ and subrings of $A$ containing $C_0$.

This has already been done successfully in the special cases (1), (2), (3), listed above—for division rings by Cartan [3] and Jacobson [9], for simple rings with minimum condition by Hochschild [6] and Nakayama [15], and for completely primitive rings by Dieudonné [5] and Nakayama [15]. An excellent exposition and revision of these results is found in a book by Jacobson soon to appear in the Colloquium series of the American Mathematical Society. The authors are particularly indebted to Professor Jacobson for the use of the manuscript of this book.

In all these special cases, except when $A$ is a field, the Galois correspondence does not pair off an arbitrary subgroup with an intermediate ring. For example, if $\Gamma$ is a subgroup of $\Gamma_0$ paired with a subring $C$ of $A$ then we want $\Gamma$ to consist of all automorphisms of $A$ over $C$. This imposes the following condition on $\Gamma$: if $I_x$ and $I_y$ are inner automorphisms (by $x$ and $y$) lying in $\Gamma$, i.e., if $x$ and $y$ commute elementwise with $C$, then $I_{x+y}$ (if it exists) must also be in $\Gamma$. A group satisfying this condition is called *complete* (cf. (4.2)). A

Presented to the Society, September 2, 1954; received by the editors September 11, 1954.

(1) This paper was written while the authors held a grant from the National Science Foundation.

counterexample due to Teichmüller [6, p. 298] shows that except in case of division rings yet another hypothesis must be added (4.4). Following Hochschild [6, p. 295] and Nakayama [15, p. 281], we combine these two conditions with our finiteness assumptions in the definition of a regular group (§4). We also restrict the class of intermediate rings to be continuous transformation rings (even in the classical theory of fields we restrict ourselves to intermediate rings which are fields) satisfying a simple condition dictated by the Teichmüller counterexample.

As soon as Artin's approach to Galois theory is adopted, it becomes clear that the first natural object of study is not the group $\Gamma_0$ of automorphisms of $A$ but a related ring $B_0$ of endomorphisms of $M$: If $\gamma \in \Gamma_0$ then the automorphism $a \to a\gamma$ can be effected by an inner automorphism $a \to s^{-1}as$ of the ring of endomorphisms of the additive group $M$ where $s$ and $s^{-1}$ are continuous $D$-semilinear transformations [11, p. 266]. However $s$ is not unique, it is arbitrary to the extent of multiplying (on either side since $s$ is semilinear) by a scalar operator in $D$. Thus the elements $\gamma$ in $\Gamma_0$ pair off in a 1-1 manner with certain one-dimensional $D$-spaces of continuous endomorphisms: $B(\gamma) = sD$. $B_0$ is the sum $\sum_{\gamma \in \Gamma_0} B(\gamma)$, which to a large extent substitutes for $\Gamma_0$.

In some respects $B_0$ is a simpler object than $\Gamma_0$ since it consists of operators on $M$ (just as $A$ already does) rather than operators on the ring of operators $A$. §4 is devoted to the relation between $B$'s and $\Gamma$'s, the principal 1-1 correspondence being enunciated in Theorem 2.

The ring $C_0$ of invariants under $\Gamma_0$ is easy to locate in terms of $B_0$. Indeed, $C_0$ is the centralizer (commuting ring) of $B_0$ in the ring of all continuous endomorphisms of the additive group $M$. Thus we are led to study centralizers of certain rings of continuous endomorphisms. §3 is devoted to this subject, the fundamental centralizer theorem being Theorem 1. The full force of this theorem is not actually needed for the Galois theory proper. A specialized version sufficient for these purposes has already been studied by one of us [16]. However, Theorem 1 is of independent interest. In the special case (3) above, it (together with Proposition 2) reduces to the Jacobson-Bourbaki theorem [3, p. 63].

The Galois correspondence (Theorem 3, §5) then appears as the composite of the two correspondences: automorphism groups $\leftrightarrow$ endomorphism rings and endomorphism rings $\leftrightarrow$ continuous transformation rings.

Besides the Galois correspondence, §5 contains two other theorems of standard type: one (Theorem 4) on extension of isomorphisms, whose proof, once we are given our Theorem 1, follows closely the lines of Nakayama's proof of the corresponding theorem for simple rings with minimum condition [15, Lemma 1.3]; and one (Theorems 5 and 5′) giving necessary and sufficient conditions for an intermediate ring to be Galois (normal) over the base ring (cf. the discussion before Theorem 5).

2. **Notations and background.** In this section we gather together the basic facts we need on dual spaces, weak topology, primitive rings with minimal one-sided ideals, and completely reducible modules. We also establish the notations that will be used in the rest of the paper.

Throughout this paper $M$ and $N$ will denote a fixed pair of dual vector spaces over a division ring $D$. That is, $M$ is a right vector space over $D$ and $N$ is a total (left) subspace of the full dual of $M$. (Cf. [4, pp. 61–63] where our remarks on dual spaces and weak topology are to be found.) Given $M$ and $N$ there is an associated weak topology on $M$, a subbase at zero consisting of the kernels of the functionals in $N$. The resulting topological vector space is said to be *weakly topologized*. (A weak topology on a vector space $M$ over $D$ could be defined independently of $N$ in the following manner: a subbase at 0 is a specified collection of subspaces of finite codimension with zero intersection.) $N$ can also be retrieved from the topology: $N$ is exactly the set of all continuous linear functionals from $M$ to $D$, with $D$ carrying the discrete topology. This topology behaves in special ways relative to vector subspaces:

(2.1) *Every weakly topologized finite-dimensional vector space is discrete. In particular, if $V$ is a finite-dimensional subspace of a weakly topologized space, $V$ is discrete and closed.* Since the subspace neighborhoods of zero in $V$ satisfy the minimum condition, their intersection is 0 only if some finite intersection is already 0, which makes the point 0 open. If $V$ is a subspace of $M$ then the induced topology on $V$ is indeed a weak topology and so $V$ is discrete, hence complete, hence closed in $M$.

(2.2) *If $M$ is weakly topologized, a vector subspace $W$ of $M$ is open (is a neighborhood of zero) if and only if it is closed and has finite codimension.* "If": $M/W$ is discrete by (2.1) and $W$ is the inverse image of the open set 0 in $M/W$. "Only if": Any open subgroup $W$ of a topological group is the complement of a union of open cosets of $W$, hence is closed. Furthermore $W$ contains a neighborhood $V$ of 0 which is a finite intersection of kernels of functionals. Thus $V$ and $W$ have finite codimension.

For the sake of completeness we also remark that a vector subspace is closed if and only if $W$ is its own double annihilator: $W$ = the set of all vectors in $M$ which are mapped on 0 by all functionals in $N$ which map $W$ on 0.

We make the following notational conventions: All function symbols will be written on the right, e.g. $Mf$ will denote the images of all the vectors in $M$ under the mapping $f$, and consequently the product $fg$ of two functions will denote the result of first applying $f$ and then $g$. If $m \in M$ and $n \in N$ then instead of $mn$ for the image in $D$ associated to $m$ by the functional $n$ we use the more established notation $(m, n)$. If $B$ is a collection of functions on a set $M$ and $U \subset M$, we use $B \mid U$ to denote the collection of restrictions of the functions in $B$ to $U$. Finally, if $C$ is a subring of $A$ we use $A(C)$ to denote the centralizer of $C$ in $A$: the set of all elements in $A$ which commute with every element of $C$.

This paper is concerned almost exclusively with rings of endomorphisms of the additive group $M$. We denote by $E$ the ring of all such endomorphisms and by $E_c$ the ring of all continuous endomorphisms. In particular each scalar in $D$ produces an endomorphism on $M$ which we identify with that scalar; in other words we shall assume $D \subset E$ (and in fact $D \subset E_c$ since the neighborhoods of 0 are $D$-spaces).

Our main object of study is the ring $A = \mathcal{L}(M, N)$ of all continuous linear transformations on the weakly topologized vector space $M$. A linear transformation $a$ on $M$ is continuous if and only if for every $f$ in $N$ the functional $m \to (ma, f)$ is again an element of $N$ [10, Lemma 3]. If this is the case we denote this functional by $fa^*$ so that

$$(ma, f) = (m, fa^*)$$

and $a^*$ becomes a linear mapping on $N$. It is trivial to verify that $a \to a^*$ is an anti-isomorphism of $A$ onto a ring of operators on $N$.

In the sequel we shall have to consider a class of rings somewhat more general than continuous transformation rings; namely primitive rings with minimal right ideals (abbreviated to P.M.I. rings), and accordingly we list some of their properties here. If $A$ is a P.M.I. ring, there exists a pair of dual vector spaces $(M, N)$ over a division ring $D$ such that $\mathcal{F}(M, N) \subset A \subset \mathcal{L}(M, N)$ where $\mathcal{F}(M, N)$ is the ring of all continuous finite-valued(2) linear transformations on the weakly topologized space $M$ [10, Theorem 8]. $\mathcal{F}(M, N)$ is also equal to the sum of all the minimal right ideals in $A$. It is a simple ring and in fact is the minimal two-sided ideal in $A$, called the socle of $A$ [8, p. 317].

If $A$ is a P.M.I. ring both $M$ and its topology (i.e. both $M$ and $N$) can be obtained from $A$ in the following manner:

(2.3) *$M$, as a faithful irreducible right $A$-module, is $A$ isomorphic to any other such module; e.g. $M$ is $A$-isomorphic to any minimal right ideal of $A$ ($D$ of course is the set of $A$-endomorphisms of $M$)* [8, p. 318].

(2.4) *A vector subspace $W$ of $M$ is open (is a neighborhood of 0) if and only if it is the kernel of a socle element of $A$.* If $e$ is in the socle of $A$, $Me$ is finite-dimensional and so discrete by (2.1). Thus the kernel of $e$, being the inverse image of the open set 0, is open. Conversely if $W$ is an open subspace, let $V$ be a complement of $W$. Then, by (2.2), $V$ is finite-dimensional and so the projection of $M$ on $V$ along (i.e. annihilating) $W$ is an element of $\mathcal{F}(M, N)$ with kernel $W$.

Since by (2.3) any faithful irreducible right $A$-module $M'$ is $A$-isomorphic to $M$, it follows that if we topologize $M'$ by letting the neighborhoods of 0 be the kernels of socle elements, we obtain a topological vector space homeomorphic to $M$. We shall speak of this topology as the weak topology that $A$ induces on a faithful irreducible right module.

The hypothesis P.M.I. is actually right-left symmetric: a P.M.I. ring

(2) I.e. having a range which is a finite-dimensional vector space over $D$.

also has minimal left ideals whose sum is the socle [10, p. 13]. There is only one faithful irreducible left $A$-module and so if $A$ is a P.M.I. ring with $\mathfrak{F}(M, N) \subset A \subset \mathfrak{L}(M, N)$, $N$ is $A$-isomorphic to any faithful irreducible left $A$-module.

We shall have much occasion to deal with completely reducible modules as well as irreducible ones. The standard results are the following [14, pp. 63–66]:

Let $G$ be a collection of endomorphisms of an abelian group $P$, so that $P$ is a $G$-module. Without loss of generality $G$ may be taken to be a ring: If $G$ is not a ring, replace it by the ring of endomorphisms it generates. $P$ is called completely reducible—we shall sometimes refer to $G$ as completely reducible—in case $P$ is a sum of irreducible $G$-modules. In this case $P$ is the direct sum of some of these irreducible modules. Every submodule has a complementary submodule and is itself completely reducible. If $P$ is expressed as a direct sum of irreducible submodules, then every irreducible submodule is isomorphic to one of the direct summands.

The cardinal number of direct summands is an invariant which is called the dimension of $P$ over $G$ and is denoted by dim $(P/G)$. In an important special case we use a slightly different notation for this dimension: If $P$ is a ring with unit and $G$ a division subring with the same unit (or rather $G$ is the ring of right multiplication on $P$ by the elements of the division subring) then $P$ is a completely reducible (right) $G$-module whose dimension we write as $[P:G]_r$ or just as $[P:G]$ if $G$ is in the center of $P$.

(2.5) *If $P$ is a completely reducible $G$-module then every finitely generated submodule has finite dimension and conversely.* (Thus "finite submodule" may be used unambiguously for either of these concepts.) Since $P$ is a sum of irreducible modules, each element of $P$, and hence each finitely generated submodule of $P$, is contained in a finite sum of these irreducible modules. Such a finite sum has finite dimension and so has each of its submodules. The converse is trivial.

Let $P$ be expressed as $\sum_{\oplus} P_\alpha$ ($\sum_{\oplus}$ denotes direct sum) with $P_\alpha$ irreducible and let $P_0$ be a fixed irreducible submodule. The sum of all $P_\alpha$'s isomorphic to $P_0$ is a submodule of $P$ called a *homogeneous component* of $P$. It is actually the sum of *all* submodules of $P$ isomorphic to $P_0$. $P$ is the direct sum of all its homogeneous components. $P$ (or sometimes $G$) is called homogeneous in case there is only one homogeneous component, i.e. all the irreducible submodules of $P$ are isomorphic.

Finally, we need the following results:

(2.6) *If $C$ is a ring of endomorphisms of $M$ which is completely reducible and homogeneous and if $R$ is a nonzero right ideal in $C$, then $MR = M$.* If $M_\alpha$ is any irreducible submodule, $M_\alpha R = 0$ or $M_\alpha$. If $M_\alpha R = 0$ then $R$ annihilates every (isomorphic) irreducible submodule and so annihilates their sum contradicting $R \neq 0$. Hence $M_\alpha R = M_\alpha$ and $MR$ contains every $M_\alpha$, hence their sum, $M$.

(2.7) *If $C$ is a P.M.I. ring of endomorphisms on $M$ with socle $S$, then $M$ is a homogeneous completely reducible $C$-module if and only if $MS=M$.* If $M=MS$ then $M=\sum mR$, the sum ranging over all $m$ in $M$ and all the minimal right ideals $R$ in $C$. But $mR$ is a $C$-homomorph of $R$ and so is zero or an irreducible $C$-module. The converse is an immediate consequence of (2.6).

The result (2.7) may be found in Jacobson's forthcoming book mentioned earlier; the "if" part is already in [5, p. 158].

3. **Completely reducible rings.** In this section we study a completely reducible subring $C$ of $A=\mathfrak{L}(M, N)$ and its centralizer $E_c(C)$ in the ring of all continuous endomorphisms of $M$, i.e. the set of those continuous endomorphisms which commute with the elements of $C$. Without restrictions of continuity such studies can already be found in [17, §119] and [4, pp. 156–158]. (Of particular significance here is the so-called Jacobson-Bourbaki theorem [3, p. 53] to which our results reduce if $A$ is a division ring.) The case where the centralizer is generated by finitely many continuous semilinear transformations has already been studied by one of us in [16]. In the present section, with no mention of semilinear transformations, we are forced to treat $M$ and $N$ in an asymmetric fashion, since there is no natural way of having $E_c(C)$ act on $N$. This is the principal difference from the approach in [16, Theorem 1]. It allows us to produce a satisfactory duality theorem (Theorem 1), though, as indicated in the introduction, in the situations arising in §§4 and 5 the hypotheses used in [16] are actually fulfilled and the conclusions in [16] are sufficient to carry out our proofs.

THEOREM 1. *Let $\mathcal{C}$ be the class of all subrings $C$ of $A=\mathfrak{L}(M, N)$ satisfying the conditions*

(i) *$C$ is a continuous transformation ring with socle $S$,*

(ii) *$MS=M$,*

(iii) *$NS^*=N$,*

(iv) *$S$ is contained in the socle of $A$.*

*Let $\mathcal{B}$ be the class of all subrings of $E_c$ containing $D$ and satisfying*

(i*) *$B$ is completely primitive with socle $T$,*

(ii*) *$MT=M$,*

(iii*) *The right $D$-dimension of a minimal right ideal of $B$ is finite.*

*Then the correspondence $C\to E_c(C)$, $B\to E_c(B)$ is a* 1-1 *correspondence between $\mathcal{C}$ and $\mathcal{B}$. If $C$ in $\mathcal{C}$ and $\mathcal{B}$ in $B$ correspond then*: (1) *$B=E_c(C)=E(C)$ so that every endomorphism commuting with $C$ is continuous.* (2) *If $B$ is all linear transformations on a space of dimension $\aleph$ then the dimension of $M$ over $C$ is also $\aleph$.* (3) *$M$ is an irreducible $BC$-module.*

Before we begin the proof, we remark that if $A$ and $C$ are simple with minimum condition and have the same identity element, then (i)–(iv) are automatic. For the first part of the proof of Theorem 1 (through (3.13)) we shall use $B$ for a ring in $\mathcal{B}$, $C$ for $E_c(B)$, and shall show that $C\in\mathcal{C}$ and $E_c(C)$

$=B$. We begin with a pair of topological lemmas (3.1) and (3.2) which eliminate essentially all difficulties with continuity. These and the several succeeding lemmas may be thought of as lifting to $B$ and $C$ several of the important properties of $D$ and $A$ (note, for example, that $D=E(A)=E_c(A)$).

(3.1) *A fundamental system of neighborhoods of* 0 *in* $M$ *can be chosen so as to consist of* $B$*-modules.* Let $X$ be a $D$-space neighborhood of 0. It suffices to show that $X$ contains an open $B$-module. Let $I$ be a minimal right ideal in $B$ and $b_1, \cdots, b_n$ a basis of $I$ over $D$. Since each $b_i$ is continuous, there are neighborhoods $X_i$ of 0 with $X_ib_i \subset X$. Let $Y=\bigcap X_i$. Then $Yb_i \subset X$ and $YI = \sum Yb_iD \subset X$. Then $YI$ is a $B$-module contained in $X$. We shall show that $YI$ has finite codimension over $D$. Let $Y+F=M$ with $F$ a finite-dimensional $D$-space. Then $YI+FI=MI=M$ (2.6) so that a complement of $YI$ may be found in $FI$. But if $x_1, \cdots, x_m$ is a basis of $F$ over $D$, each $x_iB$ is a finite sum of irreducible $B$-modules (2.5) each of which is finite-dimensional over $D$, so that $FI \subset \sum x_iB$ is finite-dimensional over $D$. Thus $YI$ is a $B$-module with finite-dimensional complement and contained in $X$. A straightforward argument shows that the closure of $YI$ is also a $B$-module contained in $X$ with finite codimension, which makes it open as required (2.2).

(3.2) *Let* $U$ *be a finite* $B$*-submodule of* $M$*. Then there is an open* $B$*-module* $W$ *such that* $M=U \oplus W$. $U$ is a sum of a finite number of irreducible $B$-modules, each of which is finite over $D$. Thus $U$ is a finite $D$-space and carries the discrete topology (2.1). Then 0 is open in $U$ and so equals $U \cap W_1$ where $W_1$ is a $B$-module neighborhood of zero in $M$. Let $W_2$ be a $B$-complement of $U \oplus W_1$—which exists because (ii*) makes $M$ a completely reducible $B$-module (2.7). Then $W=W_1+W_2$ is a $B$-complement of $U$ which is open since it contains the open set $W_1$.

(3.3) *Any* $B$*-homomorphism of a finite* $B$*-submodule* $U$ *into* $M$ *can be extended to an element of* $C$. Write $M=U \oplus W$ as in (3.2) and define the extension by making it vanish on $W$. The extension is continuous because its kernel contains $W$ and so is open.

(3.4) *Every finite* $B$*-module is the image of a finite-valued idempotent in* $C$*; and, conversely, every finite-valued idempotent in* $C$ *is projection on a finite* $B$*-module.* Given a finite $B$-module $U$, $U=Me$ where $e$ is projection on $U$ along $W$ ($W$ chosen as in (3.3)). Conversely, if $e$ is finite-valued and in $C$, then $Me$ is a $B$-module finite over $D$, hence also finite over $B$.

In particular, every irreducible $B$-module is the image of a finite-valued idempotent in $C$. We shall refer to such an idempotent as an *irreducible* idempotent. It turns out that the irreducible idempotents are exactly the idempotents which generate minimal right ideals in $C$ [cf. footnote 4].

(3.5) *If* $x \in M$*, there exists a finite-valued idempotent* $e$ *in* $C$ *with* $xe=x$*. Thus if* $xe=0$ *for every finite-valued idempotent in* $C$ *(or even for every irreducible idempotent in* $C$*), then* $x=0$. Since $xB$ is a finite sum of irreducible $B$-modules, each of which is finite-dimensional, projection on $xB$ (3.4) will send

$x$ into itself. The second assertion is clear once we note that every finite-valued idempotent in $C$ is a sum of irreducible idempotents in $C$: If $U=Me$ is a finite-dimensional $B$-module, let $M=U\oplus W$ and $U=U_1\oplus\cdots\oplus U_n$ with $U_i$ irreducible, and let $e_i$ be projection on $U_i$ along

$$U_1\oplus\cdots\oplus U_{i-1}\oplus U_{i+1}\oplus\cdots\oplus U_n\oplus W.$$

Then $e_i$ is irreducible and $e=\sum e_i$.

(3.6) *Let $U$ be an irreducible $B$-module in $M$, $U=Me$ with $e$ an irreducible idempotent in $C$. Then the division ring of $B$-endomorphisms of $U$ is $eCe|U$*[3]. $eCe$ does send $U$ into $U$ and commute with $B$. Conversely, any $B$-endomorphism $\bar{c}$ on $U$ may be extended to an element $c$ in $C$ by (3.3), and then $\bar{c}=ece$.

(3.7) *If $U$ and $e$ are as in* (3.6), *then* $UC=MeC=M$. Every irreducible $B$-module in $M$ is $B$-isomorphic to $U$, hence is of the form $Uc$ for some $c$ in $C$ by (3.3). Thus $UC$ contains the sum of all irreducible $B$-submodules of $M$. Since $B$ is completely reducible, this last sum is $M$.

(3.8) $B=E_c(C)=E(C)$. Let $\overline{B}=E(C)$ and let $U=Me$ be an irreducible $B$-module with $e\in C$. Then $U$ is a $\overline{B}$-module and $\overline{B}$ induces $eCe$-linear transformations on $U$ (i.e., $\overline{B}$ commutes with $e$ and with $eCe$). Now $B$, being completely primitive, induces all linear transformations on its irreducible module, so for every $\bar{b}$ in $\overline{B}$, there is a $b$ in $B$ with $b=\bar{b}$ on $U$. Since $UC=M$ and both $b$ and $\bar{b}$ commute with $C$, $b=\bar{b}$ on $M$. Thus $B\subset E_c(C)\subset E(C)\subset B$.

This establishes half of the 1-1 correspondence of our theorem, except that we have yet to show that $C\in\mathcal{C}$. This we proceed to do.

(3.9) *$C$ contains no nilpotent ideals.* If $I$ is such an ideal and if $e$ is any irreducible idempotent in $C$, then $eIe$ is a nilpotent ideal in $eCe$. But $eCe$ is a division ring by (3.6) and Schur's Lemma (it is clear that $eCe$ is isomorphic to $eCe|U$) so $eIe=0$. Then $0=MeIe=MeCIe=MIe$. Thus $Ie=0$ for every $e$ and $I=0$ by (3.5).

(3.10) It now follows from (3.6) and (3.9) that $eC$ is a minimal right ideal[4] in $C$ [10, p. 13]. $C$ operates faithfully on $eC$ since $eCc=0$ implies $0=MeCc=UCc=Mc$, and $c=0$. Thus $C$ is a primitive ring with nonzero socle $S$. Since the socle is the sum of all the minimal right ideals, $eC\subset S$ and $M=MeC\subset MS$, proving (ii). Furthermore, $S$ contains the irreducible idempotents of $C$, which are finite-valued linear transformations. If $F$ is the socle of $A$ (=all continuous finite valued linear transformations), then $C\cap F$ is an ideal in $C$ which meets $S$. Since $S$ is a simple ring, $C\cap F\supset S$, so that $C$ satisfies (iv). As a matter of fact, $C\cap F=S$, since if an element $c$ in $C$ is finite-

---

[3] $eCe|U$ denotes the restriction of $eCe$ to $U$.

[4] This proves that if $Me$ is an irreducible $B$-module then $eC$ is a minimal right ideal in $C$. Conversely if $Me$ is reducible, then $e$ can be written as a sum of orthogonal idempotents in $eCe$ as in the proof of (3.5) and $eC$ is not minimal.

valued, then $Mc$ is a finite $B$-module, $Mc=Me$ with $e$ an idempotent in $S$, $c=ce\in S$.

(3.11) *$C$ satisfies* (iii). If $f\in N$, (3.1) asserts there is an open $B$-module $W$ contained in the kernel of $f$. Let $U$ be a $B$-complement of $W$ and $e$ the projection on $U$ along $W$. Then $e$ is a finite-valued idempotent in $C$, by (2.2) and $W=M(1-e)$. Furthermore $e$ is in $C\cap F=S$. Then $0=(W,f)=(M[1-e],f)=(M,f[1-e]^*)$ so that $f(1-e^*)=0$, $f=fe^*\in NS^*$ for every $f$ in $N$.

(3.12) *If $C$ is a P.M.I. subring of $A$ (i.e. a primitive subring with minimal ideals) with socle $S$ satisfying* (iii) *and* (iv), *then an equivalent system of neighborhoods of zero in $M$ is the collection of all kernels of elements of $S$*([5]). *Thus if $V$ is an irreducible $C$-module in $M$, the topology induced on $V$ as a subset of $M$ is the same as the weak topology $V$ carries as an irreducible module over the P.M.I. ring $C$.*

Since the elements of $S$ are in the socle of $A$ by (iv), their kernels are neighborhoods of 0 (2.4). On the other hand every neighborhood of zero is an intersection of kernels of functionals $f$ in $N$, so it is sufficient to exhibit for each $f$ in $N$ an element $e$ in $S$ whose kernel lies in the kernel of $f$. Since $NS^*=N$, $f=\sum f_is_i^*$ with $s_i\in S$ and $f_i\in N$. Choose an idempotent $e$ in $S$ such that $es_i=s_i$ for all $i$ [12, Theorem 9]. Then $fe^*=f$, so that if $W$ is the kernel of $e$, $(W,f)=(W,fe^*)=(We,f)=0$ and $W$ is in the kernel of $f$.

Therefore if $V$ is an irreducible $C$-module, the neighborhoods of 0 in the topology induced by $M$ may be taken as the kernels in $V$ of elements of $S$. By (2.4) these are precisely the neighborhoods of zero in the weak $C$-topology.

(3.13) *If $B\in\mathfrak{B}$ and $C=E_c(B)$ then $C$ is a continuous transformation ring.* Let $V$ be an irreducible $C$-module in $M$ topologized as a subset of $M$. By (3.12) this makes $V$ a weakly-topologized vector space over the commuting division ring $\Delta$ of $C|V$, and it suffices to show that $C$ induces all continuous $\Delta$-linear transformations on $V$.

$M$ is a direct sum of irreducible submodules $C$-submodules $V_\alpha$ each $C$-isomorphic to $V$ (2.7). Any isomorphism of $V$ onto $V_\alpha$ may be extended to a $C$-endomorphism $b_\alpha$ on $M$ (simply by defining $b_\alpha=0$ on a $C$-complement of $V$) so we may write $M=\sum_\oplus Vb_\alpha$ with $b_\alpha\in E(C)=B$. If we are given a $\Delta$-linear transformation $\bar{c}$ on $V$ we extend it to an endomorphism $c$ on $M$ by making it commute with each $b_\alpha$. We show first that the resulting $c$ commutes with every $b$ in $B$; for this it suffices to check the commutation on every $Vb_\alpha$. If $Vb_\alpha b=0$, then $vb_\alpha bc=0=vb_\alpha cb$ and $bc=cb$ on $Vb_\alpha$. If $Vb_\alpha b\neq 0$ then $b_\alpha b$ is an isomorphism of $V$ so that the elements of $Vb_\alpha b$ are uniquely expressible in the form $vb_\alpha b$ with $v\in V$. Since $vb_\alpha b\in M=\sum_\oplus Vb_\beta$, it is expressible as $\sum_\beta v_\beta b_\beta$ with $v_\beta$ in $V$. The mapping $v\to v_\beta$ is then a single-valued endomorphism of $V$ which commutes with $C$. Hence we may write $v_\beta=v\delta_\beta$ with $\delta_\beta$ an element of $\Delta$

([5]) In fact the coincidence of these two topologies on $M$ is equivalent to (iii) and (iv), which gives another interpretation of these two hypotheses. See also the discussion of heights and indices before Proposition 2.

independent of $v$. Then $vb_\alpha bc = \sum_\beta v\delta_\beta b_\beta c = \sum_\beta v\delta_\beta \bar{c} b_\beta = \sum_\beta v\bar{c}\delta_\beta b_\beta$ since $\bar{c}$ is $\Delta$-linear. On the other hand, $vb_\alpha cb = v\bar{c}b_\alpha b = \sum_\beta v\bar{c}\delta_\beta b_\beta$, proving $cb = bc$.

If $\bar{c}$ is continuous, then $c$ is also continuous: If $W$ is any neighborhood of 0 in $M$—$W$ may be chosen as the kernel of an $e$ in $S$—we are to find a kernel $W_1$ of an $e_1$ in $S$ such that $W_1 c \subset W$. Now $W \cap V$ is a neighborhood of 0 in $V$ and since $\bar{c}$ is continuous on $V$ we may find $e_1$ in $S$ with kernel $W_1$ such that $(W_1 \cap V)\bar{c} \subset W \cap V$. Now let $x = \sum v_\alpha b_\alpha \in W_1$ with $v_\alpha \in V$. Then $0 = xe_1 = \sum v_\alpha b_\alpha e_1 = \sum (v_\alpha e_1) b_\alpha$ so that $v_\alpha e_1 = 0$ for all $\alpha$ (since $\sum Vb_\alpha$ is a direct sum). But then $v_\alpha \in W_1 \cap V$ so that $v_\alpha \bar{c} \in W \cap V$, $v_\alpha \bar{c} e = 0$, $0 = \sum v_\alpha \bar{c} e b_\alpha = \sum v_\alpha b_\alpha ce = (xc)e$ and $xc \in W$.

This proves $c \in E_c(B) = C$, proving (3.13).

(3.8), (3.10), (3.11), and (3.13) prove the first half of our 1-1 correspondence.

Next we start with a $C$ that is assumed to satisfy conditions (i)–(iv) and prove that its centralizer in $E_c$ is a ring in $\mathfrak{B}$ and the double centralizer of $C$ is again $C$.

(3.14) *If $C$ is a P.M.I. ring satisfying* (ii), (iii), (iv) *then* $E(C) = E_c(C)$. The neighborhoods of zero in $M$ are the kernels of elements of $S$ (3.12), and so are $E(C)$-modules. Hence each element $b$ in $E(C)$ sends each neighborhood of 0 into itself, which makes $b$ continuous, so that $E(C) \subset E_c(C)$. The reverse inclusion is obvious.

(3.15) *If $C \in \mathfrak{C}$ and $B = E_c(C)$, then $B \in \mathfrak{B}$.* Since $B = E(C)$, and $C$ is a completely reducible, homogeneous ring of endomorphisms on $M$ by (i), (ii), (2.7), and (2.3), standard computations show that the $C$-endomorphisms of $M$ (i.e. $E(C)$) form a completely primitive ring which is completely reducible on $M$ [5, pp. 156–157]. Thus $B$ satisfies (i*) and (ii*). Since $C \subset A$, $B$ clearly contains $D$. As for (iii*), let $e$ be an element of the socle of $C$. $Me$ is a $B$-module finite-dimensional over $D$ by (iv). Any irreducible $B$-submodule of $Me$ is then also finite over $D$. But all irreducible $B$-modules (including the minimal right ideals of $B$) are $B$-isomorphic, hence $D$-isomorphic, hence finite over $D$.

(3.16) *If $C$ and $B$ are as in* (3.15), *if the dimension of $M$ over $C$ is $\aleph$ and $B$ is isomorphic to all linear transformations on an $\aleph'$-dimensional space, then $\aleph = \aleph'$.* This is also a result of the computation in [5, pp. 156–157].

(3.17) *If $C \in \mathfrak{C}$ and $B = E_c(C)$, then $C = E_c(B)$.* Let $V$ be an irreducible $C$-module in $M$. Since $M$ is a completely reducible $C$-module, we can find a projection $\eta$ of $M$ on $V$ which commutes with $C$, hence is in $B$ by (3.14)(6). Exactly as in (3.2) and (3.6) we prove that the centralizer of $C$ on $V$ is $\eta B \eta \mid V$ so that $C \mid V$ consists of continuous $\eta B \eta$-linear transformations. Since $C$ is a continuous transformation ring, it induces all linear transformations which are continuous in the weak topology of $V$ as a $C$-module; by (3.12) this is the same as the topology $V$ has as a subset of $M$. This allows us to carry over the

(6) This yields: Every $C$-module is closed since it is the kernel of a continuous idempotent.

proof of (3.8) with $C$ replacing $B$ and $V=M\eta$ replacing $U=Me$ on which $B$ induced all $eCe$-linear transformations.

(3.15) and (3.17) complete the proof of the 1-1 correspondence. Conclusions (2) and (1) of Theorem 1 are (3.16) and either (3.8) or (3.14). As for conclusion (3), if $x\in M$ then $xB$ is a sum of irreducible $B$-modules each of which, multiplied by $C$, gives $M$ by (3.7). Thus $xBC=M$. This completes the proof of Theorem 1.

For later reference we append three lesser propositions that shed somewhat more light on the nature of Theorem 1.

First, Theorem 1 remains true if we expand $\mathfrak{B}$ to the class of all complete direct sums of completely primitive rings satisfying (ii*) and (iii*), and $\mathfrak{C}$ to the class of all complete direct sums of continuous transformation rings which satisfy (ii) and (iii) and whose direct summands satisfy (iv).

In Theorem 5′ we actually have need of a specialization of this generalization which we state as Proposition 1. The proof of the full generalization runs along similar lines.

PROPOSITION 1. *Let $B$ be a semisimple subring of $E_c$ containing $D$ with $[B:D]_r<\infty$ (so that $B$ satisfies the minimum condition, is completely reducible on $M$, and satisfies* (iii*) *as well) and let $C=E_c(B)$. Then $E(C)=E_c(C)=B$.*

**Proof.** The proof follows (3.1)–(3.6) verbatim. The proof of (3.7) now shows that $UC$ is a full homogeneous component of the $B$-module $M$. If $B=\sum_{\oplus}B_i$ is the direct sum decomposition of $B$ into simple rings, it is clear that the homogeneous components of $M$ are the $MB_i$. The proof of (3.8) may now easily be adapted to prove Proposition 1: If $U$ is any irreducible $B$-module, $U\subset MB_i$ for some $i$, $B|U=B_i|U$ is all $eCe$-linear transformations on $U$ and so if $\overline{B}=E(C)$, every element $\bar{b}$ of $\overline{B}$ is matched by an element $b_i\in B_i$ on $U$. It follows that $\bar{b}=b_i$ on $UC=MB_i$. Now let $b=\sum b_i$. Then $\bar{b}=b$ on every $MB_i$, hence on $M$. Thus $\overline{B}=B$.

In the course of Theorem 1 and Proposition 1 we had occasion more than once to deal implicitly with the concepts called "index" and "height" by Dieudonné [5, pp. 159–160]. His discussion was carried out only for completely primitive rings, but it carries over essentially verbatim to a somewhat more general situation:

DEFINITION. If $A$ is a P.M.I. ring and $C$ is a P.M.I. subring, then the *index* of $C$ in $A$, $i(A:C)$, is defined thus: If $R=eC$ is a minimal right ideal in $C$, $i(A:C)=\dim\ (RA/A)$.

By a standard computation in [2, p. 102] the index is independent of the choice of $R$. The index, of course, is defined when and only when $RA$ is completely reducible as an $A$-module, which means by (2.7) $RA=RAF=eF\subset F$, where $F$ is the socle of $A$. In other words $i(A:C)$ exists if and only if $C$ satisfies (iv). When the index is defined, it is finite because every principal right ideal in $F$ has finite dimension over $A$.

DEFINITION. If $A$ is a P.M.I. ring and $C$ is a P.M.I. subring, then the *height* of $A$ over $C$, $h(A:C)$, is the $C$-dimension of a minimal right ideal of $A$, or, for that matter, of any faithful irreducible $A$-module.

$h(A:C)$ is defined when and only when a faithful irreducible $A$-module $M$ is completely reducible over $C$—i.e. when and only when $C$ satisfies (ii). $h(A:C)$ is what is called the right height in [5]. The left height is defined similarly using left ideals and exists if and only if $C$ satisfies (iii).

(3.18) *If $C$ is a division ring, $h(A:C)$ is just the $C$-dimension of a minmal right ideal of $A$.*

(3.19) *If $C$ is a division ring containing the unit of $A$ and $i(A:C)$ is defined, $A$ is a simple ring with minimum condition and $i(A:C)$ is independent of $C$ and equals the dimension of the vector space on which $A$ induces all linear transformations.*

PROPOSITION 2. *Under the hypotheses of Theorem* 1, $i(A:C)=h(B:D)<\infty$. *If $B$ is a simple ring with minimum condition besides, then also* $h(A:C)=i(B:D)$ *and* $h(A:C)i(A:C)=[B:D]_r<\infty$.

**Proof.** To compute $i(A:C)$, consider a minimal right ideal $eC$ in $C$. Then by (iv), $eF=eA=eCA$ is a direct sum $\sum_{\oplus} e_iA$ of $i(A:C)$ minimal right ideals in $A$ whose generators $e_i$ may be chosen as orthogonal idempotents with $e=\sum e_i$. Then $Me=\sum Me_i$ is a direct sum of one-dimensional $D$-spaces [10, p. 15], so that dim $(Me/D)=i(A:C)$. On the other hand $Me$ is an irreducible $B$-module (footnote 4), hence is $B$-isomorphic and so $D$-isomorphic to a minimal right ideal in $B$; therefore dim $(Me/D)=h(B:D)$. Thus $i(A:C)=h(B:D)$ and (iii*) and (3.18) assert that $h(B:D)<\infty$.

If $B$ is simple with minimum condition, then according to (3.19), conclusion (2) of Theorem 1 is exactly the equality $h(A:C)=i(B:D)$. Finally $h(A:C)i(A:C)=i(B:D)h(B:D)=$ the number of minimal right ideals in a direct decomposition of $B$ multiplied by the right $D$-dimension of each such ideal $=[B:D]_r$.

Our last observation concerns three continuous transformation rings in place of two. Up to now we have referred to a ring $C$ as satisfying (i)–(iv) of Theorem 1, $A$ being understood as fixed. Perhaps it would have been better to refer to the pair $(A, C)$ as satisfying the conditions. We shall use this terminology in

PROPOSITION 3. *Let $A$, $C$, and $C_0$ be continuous transformation rings with $A\supset C\supset C_0$ and suppose the pair $(A, C_0)$ satisfies* (i)–(iv) *of Theorem* 1. *Then so also do $(A, C)$ and $(C, C_0)$. Also $h(A:C_0)=h(A:C)h(C:C_0)$ and $i(A:C_0)=i(A:C)i(C:C_0)$, so that if $h(A:C_0)$ is finite, so are $h(A:C)$ and $h(C:C_0)$.*

**Proof.** We first prove an elementary lemma.

(3.20) *Let $R=\mathcal{L}(P, Q)$ be a continuous transformation ring on the pair of dual spaces $(P, Q)$. Then if $g$ is an idempotent in $R$, $gRg$ is again a continuous*

*transformation ring isomorphic to* $\mathfrak{L}(Pg, Qg^*)$. Clearly for any $r$ in $R$, $grg$ induces an element of $\mathfrak{L}(Pg, Qg^*)$ on $Pg$. Conversely if $r'$ is an element of $\mathfrak{L}(Pg, Qg^*)$ it can be extended to an element of $gRg$ by setting $Pgr = Pgr'$, $P(1-g)r = 0$. Hence the restriction of $grg$ to $Pg$ produces an isomorphism of $gRg$ onto $\mathfrak{L}(Pg, Qg^*)$.

Now let $e$ be an idempotent in the socle of $C_0$, then by (iv) it is also in $F$ and so $Me$ is finite-dimensional over $D$. Thus $eAe$ is isomorphic to $\mathfrak{L}(Me, Ne^*)$, a simple ring with minimum condition. Now $C$ is a continuous transformation ring $\mathfrak{L}(P, Q)$, $P$, $Q$ dual spaces over $\Delta$, and so $\mathfrak{L}(Pe, Qe^*)$ is isomorphic to $eCe$. If $Pe$ were infinite-dimensional over $\Delta$, $eCe$ would contain an infinite number of orthogonal idempotents [13, p. 63], contradicting $eCe \subset eAe$. Thus $Pe$ is finite-dimensional over $\Delta$ and $e$ is in the socle of $C$. Hence $S_0 \cap S$ is a nonzero two-sided ideal in the simple ring $S_0$ and so $S_0 \cap S = S_0 \subset S$, so that $C$ satisfies (ii), (iii). Finally since $S_0 \subset F$, $S \cap F$ is a nonzero two-sided ideal in the simple ring $S$ and so $S \cap F = S \subset F$ and (iv) is also satisfied by $C$. This proves that $(A, C)$ satisfies (i)–(iv) and $(C, C_0)$ satisfies (iv). To show $(C, C_0)$ satisfies (ii) it suffices to show that any one irreducible $C$-module $V$ is completely reducible as a $C_0$-module (2.3). This is automatic if we choose $V \subset M$ since $MS_0 = M$ by assumption and so $V$ is a submodule of a completely reducible $C_0$-module. The proof that $(C, C_0)$ satisfies (iii) is similar with $N$ (a typical irreducible left $A$-module) replacing $M$.

Now that all heights and indices are known to exist, the multiplicative behavior of heights and indices is a trivial consequence of the definitions, which completes the proof of Proposition 3.

4. **Endomorphism rings and groups.** The major part of the work involved in the Galois theory consists in developing in more detail the connection between automorphism groups on $A$ and endomorphism rings in $E_e$ that was sketched in §1.

The methods we use were originally developed by Nakayama [15] in somewhat different form. Our exposition follows closely the treatment in Jacobson's forthcoming book, with some minor improvements. Since this book is not yet available it seems best to give in detail those parts that are needed.

It is well known [11, p. 266] that every automorphism $\gamma$ of $A$ is of the form $a \to s^{-1}as$ with $s$ and $s^{-1}$ continuous semilinear transformations; and conversely. The pairing of automorphisms on $A$ and semilinear transformations on $M$ is formalized in the next two definitions:

DEFINITION. If $s$ is a continuous semilinear transformation having a continuous inverse, define $\Gamma(s)$ to be the automorphism $a \to s^{-1}as$ of $A$. If $B$ is a ring of continuous endomorphisms, define $\Gamma(B)$ to be the group of all automorphisms $\Gamma(s)$ with $s$ ranging over the semilinear transformations which are units in $B$.

DEFINITION. If $\gamma$ is an automorphism of $A$, define $B(\gamma)$ as the set of all

continuous semilinear transformations $s$ on $M$, such that $s$ and $s^{-1}$ are continuous and $\Gamma(s)=\gamma$. If $\Gamma$ is a group of automorphisms of $A$, define $B(\Gamma) = \sum_{\gamma\in\Gamma} B(\gamma)$.

Several elementary properties of $B(\gamma)$ and $\Gamma(s)$ are clear:

(4.1) $B(\gamma)=sD=Ds$ *where* $s$ *is any nonzero element of* $B(\gamma)$;

$$\Gamma(ss') = \Gamma(s)\Gamma(s').$$

As for $B(\Gamma)$ and $\Gamma(B)$, our aim in this section is to establish the fact that under suitable conditions $B\to\Gamma(B)$; $\Gamma\to B(\Gamma)$ is a duality between automorphism groups $\Gamma$ and rings $B$. More explicitly the groups and rings we consider are described in the definition below.

DEFINITION. If $\Gamma$ is a group of automorphisms of $A$ we define $T_\Gamma$ as the subring generated by the linear transformations $s$ with $\Gamma(s)\in\Gamma$ (equivalently the set of all finite sums of such $s$'s). (Note that $T_\Gamma$ contains the center of $A$ which is a field.) The corresponding set of $\Gamma(s)$ will be denoted by $\mathrm{I}_\Gamma$; it is the set of inner automorphisms of $A$ that lie in $\Gamma$ and is a normal subgroup of $\Gamma$.

DEFINITION [6, p. 295], [15, p. 281]. A group $\Gamma$ of automorphisms of $A$ is called *regular* in case:

(4.2) If $s$ is any element in $T_\Gamma$, then $\Gamma(s)$ is already in $\Gamma$ (this is the completeness hypothesis of §1).

(4.3) The index $[\Gamma:\mathrm{I}_\Gamma]$ of $\mathrm{I}_\Gamma$ in $\Gamma$ and the dimension $[T_\Gamma:Z]$ of $T_\Gamma$ over the center of $Z$ of $A$ are both finite. The product of these two integers is called the *reduced order* of $\Gamma$.

(4.4) $T_\Gamma$ is a simple ring (the hypothesis dictated by Teichmüller's counterexample [6, p. 298]).

DEFINITION. We let $\mathfrak{B}_0$ denote the class of rings $B$ satisfying

(4.5) $B$ is a simple subring of $E_c$ containing $D$, and having finite right dimension over $D$ (thus $B$ satisfies the minimum condition).

(4.6) $B$ is spanned over $D$ by semilinear transformations(7).

(4.7) $A\cap B$ is simple.

Note that $\mathfrak{B}_0$ is a subclass of the class $\mathfrak{B}$ of endomorphism rings considered in §3.

THEOREM 2. $B\to\Gamma(B)$, $\Gamma\to B(\Gamma)$ *establish a* 1-1 *correspondence between the regular automorphism groups* $\Gamma$ *and the rings* $B$ *in* $\mathfrak{B}_0$. *If* $B\leftrightarrow\Gamma$ *then also*

$$[B:D]_r = \textit{reduced order of } \Gamma,$$
$$A \cap B = T_\Gamma.$$

We start with a group $\Gamma$ of automorphisms of $A$ and write $B=B(\Gamma)$. We shall only impose the regularity hypotheses on $\Gamma$ as they become necessary. Then

(4.8) $B$ *is a subring of* $E_c$ *containing* $D$.

(7) (4.5) and (4.6) are equivalent to the condition that $E_c(B)$ is weakly Galois (weakly normal) in the sense of [5] and [15].

(4.9) *$B$ is spanned over $D$ by the semilinear transformations in the $B(\gamma)$'s; these semilinear transformations are units in $B$ because of* (4.1).

We capitalize further on the fact that $B(\gamma)=sD=Ds$: Each $B(\gamma)$ is a double $D$-module with $D$ operating by multiplication on both right and left. But $B(\gamma)$ is irreducible (one-dimensional) as a one-sided module, hence irreducible as a double module. Thus $B=\sum B(\gamma)$ is a completely reducible (double) module, and the standard theory of such modules applies. Every irreducible submodule is isomorphic to some $B(\gamma)$ and hence shares with $B(\gamma)$ the property of having the form $sD$. So the irreducible modules are completely described by the following

(4.10) *If $s\in B$ then $sD$ is a double module isomorphic to $B(\gamma)$ if and only if $s=s't$ with $s'\in B(\gamma)$ and $t\in A\cap B$ (and $s't\neq 0$ in the "if" part).* Let the isomorphism $\phi$ carry $s$ into $s'$ in $B(\gamma)$ where $s'$ is then a unit in $B$ and is semilinear with associated automorphism $\sigma$ on $D$. Then $(ds)\phi=ds'=s'd\sigma=[s(d\sigma)]\phi$ so that $ds=s(d\sigma)$. Since also $ds'=s'(d\sigma)$, $t=s'^{-1}s$ commutes with $D$—i.e., is linear—and is in $B$ since $s'^{-1}$ and $s$ are. The converse is trivial.

Note that $t$ is in general a nonunit in $A\cap B$. If $t$ is a unit then $sD$ is always a $B(\gamma)$.

(4.11) *Every irreducible submodule of $B$ is of the form $sD$, with $s$ a semilinear transformation. Every semilinear transformation belonging to $B$ is of the form $s't$ with $s'\in B(\gamma)$ for some $\gamma$ in $\Gamma$ and $t\in A\cap B$.* By (4.10) an irreducible submodule is generated by $s't$ and $s't$ is semilinear. Conversely, if $s$ is semilinear, then $sD$ is a double submodule, necessarily irreducible, hence isomorphic to some $B(\gamma)$ and (4.10) applies.

(4.12) *Every double submodule of $B$ (in particular, every ideal in $B$ and every subring of $B$ containing $D$) is generated by semilinear transformations of the form $s't$ with $s'\in B(\gamma)$ and $t\in A\cap B$.* The submodule is also completely reducible, which means that it is the sum of irreducible submodules, each of which is generated by $s't$ as in (4.11).

Following the theory of completely reducible modules further, we can divide the class of $B(\gamma)$'s into isomorphism classes $I_\alpha$: if we let $B_\alpha$ be the sum of all $B(\gamma)$ in $I_\alpha$, then $B$ is the direct sum of the $B_\alpha$'s. Furthermore, $B_\alpha$ contains every irreducible submodule (a $B(\gamma)$ or otherwise) which is isomorphic to a $B(\gamma)$ in $I_\alpha$. We examine these isomorphism classes more closely.

(4.13) *Let $B(\gamma)=sD$. Then $B(\gamma')\cong B(\gamma)$ if and only if $B(\gamma')=stD$ with $t$ a unit in $A\cap B$, and in fact $t\in T_\Gamma$: this in turn is equivalent to $\gamma\equiv\gamma'$* (mod $\mathrm{I}_\Gamma$) [5, *Lemme* 2b].

By (4.10) if $B(\gamma')\cong sD$, then $B(\gamma')=s'D$, $s=s't'$, $t'$ linear. $t'$ is a unit in $B$ since $s$ and $s'$ are, so we may write $t=t'^{-1}\in A\cap B$ and have $B(\gamma')=s'D=stD$. Then $\gamma^{-1}\gamma'=\Gamma(s)^{-1}\Gamma(st)=\Gamma(t)$ is an inner automorphism in $\Gamma$, proving both $t\in T_\Gamma$ and $\gamma\equiv\gamma'$(mod $\mathrm{I}_\Gamma$). Conversely, if $\gamma\equiv\gamma'$(mod $\mathrm{I}_\Gamma$), let $\gamma=\gamma'\Gamma(t)$ with $t$ linear, and let $\gamma=\Gamma(s)$, and $s'=st^{-1}$. Then $\Gamma(s')=\Gamma(s)\Gamma(t)^{-1}=\gamma'$ so that $B(\gamma)=sD$ and $B(\gamma')=stD$ are isomorphic by (4.10).

It now follows immediately that

(4.14) *The set of isomorphism classes $I_\alpha$ is in* 1-1 *correspondence with the factor group* $\Gamma/\mathrm{I}_\Gamma$.

(4.15) *Choose* $s\in B(\gamma)\subset B_\alpha$. *Then* $B_\alpha = sT_\Gamma D$. For by (4.13),

$$B_\alpha = \sum B(\gamma') = \sum_{t\in T_\Gamma} stD = sT_\Gamma D.$$

We are almost ready now to compute $[B:D]_r$. We need only compute $[T_\Gamma D:D]_r$.

(4.16) *If $T$ is a space of linear transformations over the center $Z$ of $A$ and $\{t_\beta\}$ a set of elements in $T$ independent over $D$, then a linear combination $t$ of $\{t_\beta\}$ with coefficients in $D$ is a linear transformation if and only if the coefficients are in $Z$ (so that $t\in T$). Hence* $[TD:D]_r = [T:Z]$ [5, *Lemme* 2a]. If $t=\sum t_\beta d_\beta$ with $d_\beta\in D$ is a linear transformation, then $\sum t_\beta d_\beta d = td = dt = \sum t_\beta\, dd_\beta$ for every $d$ in $D$; $dd_\beta = d_\beta d$ from the independence of $\{t_\beta\}$ over $D$; each $d_\beta$ is in the center of $D$, which equals the center $Z$ of $A$. It follows that if $\{t_\beta\}$ is a maximal set of elements of $T$ independent over $D$ (so that $\{t_\beta\}$ is a basis of $TD$ over $D$) then $\{t_\beta\}$ spans $T$ over $Z$. Thus $[TD:D]_r \geqq [T:Z]$. Since any basis of $T$ over $Z$ spans $TD$ over $D$, $[TD:D]_r \leqq [T:Z]$. This proves (4.16).

(4.17) *If $\Gamma$ is any group of automorphisms of $A$ and $B=B(\Gamma)$, then* $[B:D]_r = [\Gamma:\mathrm{I}_\Gamma][T_\Gamma:Z] =$ *the reduced order of $\Gamma$. Hence $\Gamma$ has finite reduced order if and only if $B=B(\Gamma)$ has finite right dimension over $D$.* $B$ is the direct sum of $B_\alpha$'s, $[\Gamma:\mathrm{I}_\Gamma]$ in number by (4.14); and each $B_\alpha$ has right dimension over $D$ equal to $[T_\Gamma D:D]_r = [T_\Gamma:Z]$ by (4.15) and (4.16).

(4.18) $T_\Gamma = A\cap B$. $T_\Gamma$ is the set of all sums of linear transformations in $B(\gamma)$'s, hence $T_\Gamma\subset A\cap B$. Conversely, let $t$ be a linear transformation in $B$. Then $tD\cong 1D$ by (4.10). By the general theory of completely reducible modules, $tD$ is contained in the sum $B_\alpha$ of all $B(\gamma)$'s that are isomorphic to $1D$. (4.15) shows that this $B_\alpha$ is $1T_\Gamma D$, so that $t$ is a linear transformation in $T_\Gamma D$. Then $t\in T_\Gamma$ by (4.16).

(4.19) *If $A\cap B$ is simple, then $B$ is simple.* Let $I$ be a nonzero ideal in $B$. Since $I$ is a double submodule of $B$, (4.12) implies $I$ is generated by semilinear transformations of the form $s't$ with $s'$ a unit in $B$ and $t=s'^{-1}s$ a nonzero linear transformation in $I$. Thus $A\cap I\neq 0$. But $A\cap I$ is an ideal in the simple ring $A\cap B$, so $A\cap I = A\cap B$ contains 1. Thus $I=B$.

(4.20) *If $\Gamma$ is a complete group (i.e. satisfies* (4.2)) *and $B=B(\Gamma)$ then* $\Gamma(B)=\Gamma$. It is always true that $\Gamma(B)\supset\Gamma$. If $s$ is a semilinear transformation which is a unit in $B$ we have to show that $\Gamma(s)$ lies in $\Gamma$. By (4.11), $s=s't$, $s'\in B(\gamma)$, hence $s'$ is a unit of $B$ with $\Gamma(s')\in\Gamma$, and $t$ is an element of $A$ which must also be a unit in $B$. Thus $t$ is in $T_\Gamma$ and has a continuous inverse, so that $\Gamma(t)\in\Gamma$ by the completeness of $\Gamma$. Therefore $\Gamma(s)=\Gamma(s')\Gamma(t)\in\Gamma$.

(4.8), (4.9), (4.17), (4.18), (4.19), (4.20) show that if $\Gamma$ is regular and $B=B(\Gamma)$ then $B\in\mathfrak{B}_0$ and $\Gamma(B)=\Gamma$.

Next, let $B$ be any ring in $\mathfrak{B}_0$ and let $\Gamma=\Gamma(B)$.

(4.21) $\Gamma$ *is complete.* If $t\in T_\Gamma$, then $t$ is in $A$ and also is a sum of linear $t_i$'s

with $\Gamma(t_i)\in\Gamma$. That is, each $t_i$ is in $B$, so that $t$ is also in $B$. (This shows $T_\Gamma\subset A\cap B$.) If, furthermore, $t$ has a continuous inverse, this inverse must also be in $B$ ($B$ is a simple ring with minimum condition and any element of $B$ having no inverse in $B$ is a divisor of zero, which $t$ is not). Thus $t$ is a unit in $B$, $\Gamma(t)\in\Gamma$, and $\Gamma$ is complete.

(4.22) *$T_\Gamma=A\cap B$ is a simple finite-dimensional algebra over $Z$.* If in (4.16) we let $T=A\cap B$ we conclude that $[T:Z]=[TD:D]_r\leqq[B:D]_r<\infty$. By assumption (4.7) on $B$, $A\cap B$ is a simple algebra, now known to be finite-dimensional over $Z$. Hence every element of $A\cap B$ is a sum of units (e.g., cf. [18]). The units, by definition of $\Gamma$, generate inner automorphisms belonging to $\Gamma$, hence are in $T_\Gamma$. Thus $A\cap B\subset T_\Gamma$. The reverse inclusion is found in the proof of (4.21).

Our next step is to prove $B(\Gamma)=B$. This is essentially based on Nakayama's fundamental lemmas [15, Lemmas 1.1 and 1.4].

(4.23) *If $C=E_c(B)$, then $CD$ is a completely reducible homogeneous ring of endomorphisms on $M$.* By Theorem 1 the dimension of $M$ over $C$ equals the dimension over $D$ of a minimal right ideal in $B$, which is finite. Thus $M$ satisfies the minimum condition on $C$-submodules, and hence also on $CD$-submodules. So we may find a minimal $CD$-submodule $M_0$. Let $\{s_i\}$ be semilinear transformations which span $B$ over $D$. Then $\sum M_0s_i=\sum M_0CDs_i=\sum M_0s_iDC=M_0BC=M$, since $M$ is irreducible under $BC$ (Theorem 1). Furthermore, while each $s_i$ is not a $CD$-homomorphism, it is $C$-linear and $D$-semilinear, which is enough to guarantee that $M_0s_i$ is also an irreducible $CD$-module or zero. Thus $M$ is a sum of irreducible $CD$-modules. Since $E(CD)\subset E(C)=E_c(C)=B$ by Theorem 1, the centralizer $E(CD)$ equals

$$E_c(CD) = E_c(C)\cap E_c(D) = B\cap A$$

again by Theorem 1. By (4.22) $A\cap B$ is simple with minimum condition, hence homogeneous. But if $CD$ is completely reducible and $E(CD)$ is homogeneous so is $CD$ [5, p. 156].

(4.24) *Every semilinear transformation $s$ in $B$ is a sum of semilinear transformations which are units in $B$.*

Split $M$ into a direct sum of irreducible $CD$-modules: $M=M_1\oplus\cdots\oplus M_n$. Then $s\neq0$ on some $M_i$; say $M_1s\neq0$. Since $s$ is $C$-linear and $D$-semilinear, $M_1s$ is also an irreducible $CD$-module and we may take it as the first summand in another splitting of $M$: $M=M_1'\oplus\cdots\oplus M_n'$ with $M_1'=M_1s$. By (4.23) all the $M_i$ and $M_i'$ are $CD$-isomorphic, so we can choose isomorphisms $\phi_i$ sending $M_1$ into $M_i$ and $\phi_i'$ sending $M_1'$ into $M_i'$. Then define $t=\phi_i^{-1}s\phi_i'$ on each $M_i$ and we have an additive isomorphism on $M$, sending $M_i$ onto $M_i'$, which is $C$-linear (hence a unit in $B$) and $D$-semilinear. In fact the automorphism of $D$ associated with $t$ is the same as that associated with our original $s$. Thus $st^{-1}$ actually commutes with both $C$ and $D$, hence is in $E(CD)=E_c(CD)=A\cap B$. Since $A\cap B$ is a simple finite-dimensional algebra, every element of $A\cap B$ is a sum of units. If we write $st^{-1}=\sum t_i$ with each $t_i$ a unit in $A\cap B$,

then $s=\sum t_i t$ where each $t_i t$ is a unit in $B$ and also a semilinear transformation.

(4.25) *If $B\in\mathcal{B}_0$ and $\Gamma=\Gamma(B)$, then also $B=B(\Gamma)$.* It is clear that $B(\Gamma)\subset B$. For the inverse inclusion it suffices to show that every element in $B$ is spanned over $D$ by elements in $B(\gamma)$'s. The elements in $B(\gamma)$'s are the semilinear transformations which are units in $B$. The space they span over $D$ contains all semilinear transformations in $B$ by (4.24), hence all elements of $B$, by (4.6).

We can now appeal to (4.17) to guarantee that the reduced order of $\Gamma$ equals $[B:D]_r$ which is finite. This completes the proof that $\Gamma$ is regular and $B=B(\Gamma)$ and thus also completes the proof of Theorem 2.

For later applications we need to consider the following generalization of the concept of regular group:

DEFINITION. A group $\Gamma$ of automorphisms of $A$ is said to be *semi-regular* if it satisfies (4.2), (4.3) and, in place of (4.4), $T_\Gamma$ is a semisimple ring.

With the exception of (4.23) and (4.24) all the definitions and lemmas of this section carry over to semi-regular groups provided the word simple is replaced by semisimple throughout. Even part of (4.23) still remains true: $CD$ is still a completely reducible module but will be homogeneous if and only if $\Gamma$ is actually regular, i.e. if $T_\Gamma$ is simple. However (4.24) is definitely false as is shown by the Teichmüller counterexample [6].

In particular then we may state the following, which we shall need in Theorem 5′:

(4.26). *If $\Gamma$ is a semi-regular group and $B=B(\Gamma)$, then $\Gamma=\Gamma(B)$.*

5. **Galois theory.** We are now in a position to combine the results of the preceding two sections to obtain the usual 1-1 correspondence between groups and rings which constitutes the Galois theory proper. To this end we have the following

DEFINITIONS. If $\Gamma$ is a group of automorphisms on $A$, the *fixed ring* under $\Gamma$ is the set of all $a$ in $A$ with $a\gamma=a$ for all $\gamma$ in $\Gamma$.

If $C$ is a subring of $A$, the *Galois group* of $A$ over $C$ is the set of all automorphisms of $A$ which are the identity on $C$.

A ring $A$ is *Galois* over a subring $C$ if $C$ is the fixed ring under a regular group.

The first two definitions are merely restatements of situations already encountered, namely:

(5.1) *The fixed ring under a group of automorphisms $\Gamma$ of $A$ is $E_c(B(\Gamma))$.* Clearly $c\gamma=c$ if and only if $t^{-1}ct=c$ for each $t$ in $B(\gamma)$, so that $c\gamma=c$ for all $\gamma$ in $\Gamma$ if and only if $c$ commutes with $B(\Gamma)$.

(5.2) *The Galois group of $A$ over $C$ is $\Gamma(E_c(C))$.* Every automorphism of $A$ is of the form $\Gamma(s)$ with $s$ a semilinear transformation which is a unit in $E_c$. Now $\Gamma(s)$ is the identity on $C$ if and only if $s\in E_c(C)$. But then $s^{-1}\in E_c(C)$ and so $s$ is a unit in $E_c(C)$. Hence the Galois group is $\Gamma(E_c(C))$.

We can now state our fundamental theorem of Galois theory.

THEOREM 3. *Let $A$ be a continuous transformation ring, $\Gamma_0$ a regular group of automorphisms of $A$, and $C_0$ the fixed ring under $\Gamma_0$. Then we have the usual fixed ring-Galois group correspondence as a* 1-1 *correspondence between regular*(8) *subgroups $\Gamma$ of $\Gamma_0$ and continuous transformation subrings $C$ of $A$, containing $C_0$, and having simple centralizers $A(C)$ in $A$.*

**Proof.** In view of (5.1) and (5.2) it is clear that the Galois correspondence is simply a composite of the correspondences described in Theorems 1 and 2 and all we need to check is that the various hypotheses of these theorems are fulfilled in our present situation.

We begin by going from groups to rings. Thus let $\Gamma$ be a regular subgroup of $\Gamma_0$ and let $C=E_c(B(\Gamma))$ be the fixed ring under $\Gamma$. Since $B=B(\Gamma)$ is in the class $\mathfrak{B}_0$ of Theorem 2, $C=E_c(B)$ is a continuous transformation ring between $A$ and $C_0$ satisfying all the hypotheses of the class $\mathfrak{C}$ of Theorem 1. Also, by (4.18), $A(C)=A\cap B=T_\Gamma$ is simple and so $C$ is a ring of the type described in Theorem 3. Furthermore, by (5.2), the Galois group of $A$ over $C$ is $\Gamma(E_c(C))$ which equals $\Gamma(B)=\Gamma$ by Theorems 1 and 2. Hence half of the 1-1 correspondence has been established.

To prove the rest, we further remark that since $C_0=E_c(B(\Gamma_0))$, $C_0$ is a continuous transformation ring satisfying the hypotheses (i)–(iv) of Theorem 1. Now let $C$ be a continuous transformation ring with $A\supset C\supset C_0$. Then by Proposition 3 in §3, $C$ also satisfies (i)–(iv) and Theorem 1 shows $B=E_c(C)\in\mathfrak{B}$. If $B_0$ denotes $E_c(C_0)$, then $D\subset B\subset B_0$ and $B_0\in\mathfrak{B}_0$. This shows that $[B:D]_r<\infty$ and $B$ is spanned over $D$ by semilinear transformations. (4.12). By Theorem 1 (i*), $B$ is completely primitive which combined with $[B:D]_r<\infty$ shows that $B$ is simple with descending chain condition. Lastly, $A\cap B=A(C)$ so that, if $A(C)$ is assumed simple, $B\in\mathfrak{B}_0$. Hence the Galois group $\Gamma=\Gamma(B)$ of $A$ over $C$ is regular (Theorem 2) and by (5.1) the fixed ring under $\Gamma$ is $E_c(B(\Gamma))=E_c(B)$ by Theorem 2, which is $C$ by Theorem 1. This completes the proof of Theorem 3.

PROPOSITION 4. *If $\Gamma$ is a regular subgroup of $\Gamma_0$ and $C$ is its fixed ring, then $h(A:C)i(A:C)=$the reduced order of $\Gamma$.*

**Proof.** The reduced order of $\Gamma=[B(\Gamma):D]_r=[B:D]_r=h(A:C)i(A:C)$ by (4.17), Theorem 2 and Proposition 2.

Next we have

THEOREM 4. *Let $A$ be a continuous transformation ring and $C_0$ a Galois subring. Let $C$ be a continuous transformation subring of $A$ containing $C_0$ and $\sigma$ an isomorphism of $C$ into $A$ which is the identity on $C_0$. Then, if both $C$ and*

(8) The hypothesis that $\Gamma$ be a regular subgroup of $\Gamma_0$ actually demands only that $\Gamma$ be complete and $T_\Gamma$ be simple. The finiteness of the reduced order is automatic since $\Gamma$ is a subgroup of $\Gamma_0$ which has finite reduced order.

*$C\sigma$ have simple centralizers in $A$, $\sigma$ can be extended to an automorphism of $A$, cf.* [15, *Lemma* 1.3].

**Proof.** Let $G$ be the set of endomorphisms $g$ of $M$ satisfying $cg=g(c\sigma)$. Since $c_0\sigma=c_0$, $g$ lies in $E(C_0)=E_c(C_0)$ so that $G\subset E_c$. Hence we must find a semilinear transformation $s$ which is a unit in $G$, for then the automorphism $\Gamma(s)$ will induce $\sigma$ on $C$.

We first note that $G\neq 0$: Since $C$ and $C\sigma$ both contain $C_0$, it follows from Proposition 3 and (2.7) that $M$ is completely reducible and homogeneous both as $C$- and $C\sigma$-module. Then let $V$ be an irreducible $C$-submodule and let $V_1$ be an irreducible $C\sigma$-submodule. $V_1$ may also be regarded as a $C$-module by defining $x\bigcirc c$ to be $xc\sigma$ for each $x$ in $V_1$. Since all faithful irreducible $C$-submodules are isomorphic there is a $C$-isomorphism of $V$ onto $V_1$ which will be an endomorphism $\bar{g}$ of $V$ onto $V_1$ with $c\bar{g}=\bar{g}c\sigma$. If $K$ is a $C$-module complement of $V$, $\bar{g}$ can then be extended to a nonzero element $g$ of $G$ by setting $Kg=0$.

Now $DG\subset G$ and $GD\subset G$ so that $G$ is a double submodule of $E_c(C_0)=B(\Gamma_0)$. Thus $G$ is generated by semilinear transformations and we let $s$ be a nonzero linear transformation in $G$ with associated automorphism $\tau$ on $D$. We then make $M$ into a new $CD$-module $M^\dagger$ by defining $x\bigcirc(cd)=x(c\sigma)(d\tau)$. Then to finish the proof it will be sufficient to show that $M$ and $M^\dagger$ are isomorphic $CD$-modules, for such an isomorphism will be a semilinear transformation which is a unit in $G$. Since the set of operators induced on $M^\dagger$ by $CD$-modules is exactly $C\sigma D$, $M$ and $M^\dagger$ are both completely reducible homogeneous $CD$-modules. Moreover the nonzero $s$ chosen above is a nonzero $CD$ homomorphism of $M$ into $M^\dagger$, which must induce an isomorphism of some irreducible $CD$-submodule $W$ of $M$ onto an irreducible $CD$-submodule $W^\dagger$ of $M^\dagger$. Thus to show $M\cong M^\dagger$ we need only show $\dim(M/CD)=\dim(M^\dagger/CD)$. But

$$\dim(M/C_0)=\dim(M/CD)\dim(W/C_0)$$

and

$$\dim(M^\dagger/C_0)=\dim(M^\dagger/CD)\dim(W^\dagger/C_0).$$

Furthermore $M$ and $M^\dagger$ are identical finite $C_0$-modules so that $\dim(M/C_0)=\dim(M^\dagger/C_0)$; $W$ and $W^\dagger$ are isomorphic $CD$-modules, hence isomorphic $C_0$-modules so that $\dim(W/C_0)=\dim(W^\dagger/C_0)$, which shows $\dim(M/CD)=\dim(M^\dagger/CD)$.

The third typical theorem of the classical Galois theory consists of a statement like "The intermediate ring $C$ is Galois over the base ring $C_0$ if and only if the Galois group $\Gamma$ of $A$ over $C$ is normal in the Galois group $\Gamma_0$ of $A$ over $C_0$". This statement is not true in general even in the case of division rings: For, as is well known, the largest subgroup of $\Gamma_0$ in which $\Gamma$ can be normal is $\Lambda=\{\lambda\in\Gamma_0 \mid C\lambda=C\}$, which in general is not complete and so cannot be $\Gamma_0$.

However, for division rings this is the only difficulty in the sense that if $\Lambda'$ is the completion of $\Lambda$ in $\Gamma_0$(9), then $\Lambda'=\Gamma_0$ is a necessary and sufficient condition for $C$ to be Galois over $C_0$ [3, Théorème 3$\gamma$]. Hochschild [6, Theorem 2.5] and Nakayama [15, Theorem 7] prove $\Lambda'=\Gamma_0$ implies that $C_0$ is the fixed ring under some (not necessarily regular) group of automorphisms of $C$; and conversely, provided certain assumptions on the relation of $C$ and $C_0$ are made. Our next theorems show that in fact $\Lambda'=\Gamma_0$ implies that $C_0$ is the fixed ring under a *semiregular* group of automorphisms on $C$ so that $C(C_0)$ is semi-simple, and that conversely if $C_0$ is the fixed ring under a semiregular group of automorphisms on $C$, $\Gamma_0=\Lambda'$. In case $[D:Z]<\infty$ (including the case where $A$ is a finite-dimensional algebra) we can prove $\Gamma_0=\Lambda'$ under the sole assumption that $C_0$ is the fixed ring under any group of automorphisms of $C$.

However, even if $A$ is a finite-dimensional simple algebra one cannot expect $\Lambda'=\Gamma_0$ to imply that $C$ is Galois over $C_0$ as is shown by the following example:

Let $R$ be the field of real numbers, $K$ the field of complex numbers, $V=K\otimes_R K$, $K_1$ the ring of endomorphisms of $V$ consisting of the right multiplications on $V$ by the elements of $K\otimes 1$, $K_2$ the ring of right multiplications on $V$ by $1\otimes K$, $A$ the ring of all $R$-linear transformations on $V$, $C$ the ring of all $K_1$-linear transformations on $V$, $C_0=K_2$. $A$ is a central simple algebra of finite dimension over $R$ and $C$ and $C_0$ are simple subalgebras so that $C$ and $C_0$ are Galois in $A$ (by the classical theory [7, p. 104], $A(C)$ is a simple subalgebra such that $A(A(C))=C$, so that $C$ is the fixed ring under the regular group of inner automorphisms by units of $A(C)$, and similarly for $C_0$). But $C(C_0)$ contains $K_1$ and $K_2$ in its center, so that this center has $K_1K_2\cong K_1\otimes_R K_2$ in it and so contains two orthogonal idempotents. Thus $C(C_0)$ is not simple. Actually, by the Corollary to Theorem 5', $C(C_0)$ is semi-simple and $\Lambda'=\Gamma_0$.

THEOREM 5. *Let $A$ be a continuous transformation ring and let $C_0$ be a Galois subring with Galois group $\Gamma_0$. Further, let $C$ be a continuous transformation subring containing $C_0$, $\Lambda$ the group of all automorphisms in $\Gamma_0$ which leave $C$ setwise invariant, and $\Lambda'$ the completion of $\Lambda$ in $\Gamma_0$. Then if $\Lambda'=\Gamma_0$, $C_0$ is the fixed ring under a semiregular group of automorphisms of $C$, namely $\Lambda\,|\,C$; and $T_{\Lambda|C}=C(C_0)$ is semi-simple.*

**Proof.** We first note that $\Lambda$ restricted to $C$, which we denote by $\Lambda\,|\,C$, is the Galois group of $C$ over $C_0$, and so is complete. Indeed, by Theorem 4, any such automorphism can be extended to an element of $\Gamma_0$ and thus lies in $\Lambda$. Hence $C_0$ will be the fixed ring under a group of automorphisms of $C$ if and only if it is the fixed ring under $\Lambda\,|\,C$. But since $\Lambda'=\Gamma_0$ the fixed ring in $A$ of $\Lambda$ is $C_0$ and so $C_0$ is the fixed ring under $\Lambda\,|\,C$.

Now by Proposition 3, $C$ and $C_0$ are in exactly the same relation to each other as $A$ and $C$ are in §§3 and 4 and $h(C:C_0)<\infty$. Thus if $E$ is for the

(9) The smallest complete subgroup of $\Gamma_0$ containing $\Lambda$; the group generated by $\Lambda$ and the units of $T_\Lambda$. We note the more or less obvious facts $B(\Lambda)=B(\Lambda')$, $T_\Lambda=T_{\Lambda'}$.

moment the endomorphism ring of an irreducible $C$-module and $E(C)=D$ we have, by Proposition 2, $[E(C_0):D]_r=h(C:C_0)i(C:C_0)<\infty$. But by (4.17) the reduced order of $\Lambda|C=[B(\Lambda|C):D]_r$ and $B(\Lambda|C)\subset E(C_0)$ so that $\Lambda|C$ is of finite reduced order.

Finally we consider $C(C_0)$ and its radical $R$. $C(C_0)$ is a subalgebra of $A(C_0)$ over $Z\cap C_0$; $A(C_0)$ is finite over the center $Z$ of $A$ (4.18) and it is easily seen([10]) that $Z$ is finite over $Z\cap C_0$ so that $C(C_0)$ is a finite-dimensional algebra and $R$ is nilpotent. Since $C(C_0)\subset B_0$, $B_0R$ is a left ideal in $B_0=B(\Gamma_0)=B(\Lambda)$ and we proceed to show that it is a two-sided ideal. $B_0$ is generated by semilinear transformations $t$ where $\Gamma(t)$ is in $\Lambda$ and leaves $C$, $C_0$ and so $C(C_0)$ setwise fixed, thus producing an automorphism of $C(C_0)$. Hence $t^{-1}Rt=R\Gamma(t)=R$ and so $B_0Rt=B_0t^{-1}Rt=B_0R$, proving $B_0R$ is a two-sided ideal in the simple ring $B_0$ (Theorem 2). Since $R$ is nilpotent, $B_0R\neq B_0$. Thus $0=B_0R\supset R$, $C(C_0)$ is a semisimple finite-dimensional algebra so that $C(C_0)$ is generated by its units. But the units of $C(C_0)$ are exactly the units $c$ in $C$ with $\Gamma(c)\in\Lambda|C$, which generate $T_{\Lambda|C}$. Therefore, $T_{\Lambda|C}=C(C_0)$ is semisimple and $\Lambda|C$ is semiregular.

THEOREM 5′. *Let $A$ be a continuous transformation ring, $C_0$ a Galois subring with Galois group $\Gamma_0$, $C$ a continuous transformation subring containing $C_0$, $\Lambda$ the group of all automorphisms in $\Gamma_0$ leaving $C$ setwise fixed, and $\Lambda'$ the completion of $\Lambda$. If $C_0$ is the fixed ring of some group of automorphisms of $C$ and $C(C_0)$ is semisimple, then $\Lambda'=\Gamma_0$.*

**Proof.** As in the proof of Theorem 5 it follows that $C_0$ is the fixed ring under $\Lambda|C$. This leads us to study $B'=B(\Lambda)$ and we begin by showing that it is semi-simple. Now $B'\supset B=E_c(C)$ and so is a double $B$-module. Furthermore $B'=\sum tB$ with $\Gamma(t)\in\Lambda$ and since $C\Gamma(t)=C$ and $E_c\Gamma(t)=E_c$, it follows that $B\Gamma(t)=t^{-1}Bt=B$ so that $tB$ is a double $B$-submodule. Moreover $tB$ is irreducible, for if $tb\neq 0\in tB$, then $BtbB=tBbB=tB$ because $BbB$ is a nonzero two-sided ideal in the simple ring $B$. Thus $B'$ is a completely reducible double $B$-module. Now just as in (4.10) every irreducible double $B$-submodule is of the form $tcB$, with $\Gamma(t)\in\Lambda$ and $c$ an element of $B'$ commuting with $B$. Thus $c$ is in $E_c(B)=C$ and since it is also in $B_0$, it is in $C(C_0)$. The radical $R$ of $B'$ is a double $B$-submodule of $B'$ and so, if it is not zero, contains the module $tcB$ for some nonzero $t$ and $c$. Thus $c=t^{-1}(tc)$ lies in $R$ and so $R\cap C(C_0)$ would be a nonzero ideal in $C(C_0)$. But $B'$, being finite over $D$, satisfies the minimum condition so that $R$ is nilpotent. Then so is $R\cap C(C_0)$ contradicting the semi-simplicity of $C(C_0)$. Hence $B'$ is semi-simple.

Now $E_c(B')$ is the fixed ring of $\Lambda$ and since $E_c(B')\subset E_c(B)$ this is the same as the fixed ring of $\Lambda|C$ which as we saw is $C_0$. But then from the extended form of our centralizer theorem, Proposition 1, we have $B'=E(E_c(B'))$

([10]) The restriction of $\Gamma_0$ to $Z$ is a homomorph of $\Gamma_0/I_{\Gamma_0}$ which is finite since $\Gamma_0$ has finite reduced order. Thus $Z$ is finite over the fixed subfield $Z\cap C_0$ [1, Theorem 14].

$=E(C_0)=B(\Gamma_0)$ (so that $B'$ is actually simple) and $\Lambda'=\Gamma(B(\Lambda'))=\Gamma(B(\Gamma_0))$ $=\Gamma_0$ by (4.26) and Theorem 2.

COROLLARY. *Let $D$ be the division ring of $A$ with center $Z$. Then if $[D:Z]<\infty$, Theorem 5′ remains valid without the assumption $C(C_0)$ semi-simple.*

**Proof.** We shall show that $[D:Z]<\infty$ actually implies $C(C_0)$ semi-simple. As in footnote 10, $Z$ is a finite extension of the field $Z\cap C_0$, which lies in the center of $B_0$. But $[B_0:Z\cap C_0]=[B_0:D]_r[D:Z][Z:Z\cap C_0]$ and all three of these factors are finite, so that $B_0$ is a finite-dimensional algebra over $Z\cap C_0$. Note that $B$ is a finite-dimensional subalgebra since $Z\cap C_0\subset B\cap C=$the center $Z_B$ of $B$. Furthermore, by the argument in footnote 10 with $\Lambda\,|\,C$ replacing $\Gamma_0$ and $Z_B$ replacing $Z$, $Z_B$ is separable over $Z_B\cap C_0$. (This is the only use we make of the hypothesis that $C_0$ is the fixed ring under a group of automorphisms of $C$.) Now let $Z_0$ be the center of $B_0$ so that $B_0$ is a central simple algebra over $Z_0$. The subalgebra $BZ_0$ is a homomorph of the scalar extension $B\otimes_{Z_B\cap Z_0}Z_0$ and so is finite-dimensional and semi-simple since $B$ is finite-dimensional and separable over $Z_B\cap C_0=Z_B\cap Z_0$. The proof of the classical theorem on centralizers of simple subalgebras of a central simple algebra given in [7, p. 103] applies equally well to show that $B_0(BZ_0)$ is semi-simple. But $B_0(BZ_0)=B_0(B)=B_0\cap E_c(B)=E_c(C_0)\cap C=C(C_0)$.

In particular our corollary yields Hochschild's result [6, Theorem 2.5] without the additional hypothesis imposed there. The fact that this hypothesis is superfluous was already noted by Nakayama [15, p. 290].

In case $[D:Z]<\infty$ and $Z$ is of characteristic 0 it follows that $C(C_0)$ is semi-simple without even assuming $C_0$ is the fixed ring of $\Lambda\,|\,C$. Indeed, this hypothesis was used only to show $Z_B$ separable over $Z_B\cap C_0$, which is automatic in the case of characteristic zero.

It is plausible that, without any extra assumption, $C_0$ being the fixed ring under $\Lambda\,|\,C$ implies $C(C_0)$ semi-simple, but we have no further information on this subject.

We remark finally that if $\Lambda'=\Gamma_0$, $C(C_0)$ must be a sum of isomorphic simple ideals. For let $I$ be the sum of all simple ideals of $C(C_0)$ isomorphic to a fixed one, so that $I$ is a two-sided ideal of $C(C_0)$ setwise invariant under all the automorphisms of $C(C_0)$. Then if $I\neq C(C_0)$ there is an $e\neq 0$ in $C(C_0)$ such that $Ie=0$. But then just as in the proof of the semi-simplicity of $C(C_0)$ in Theorem 5, $B_0I=B_0$ which would yield $B_0e=0$, a contradiction.

## REFERENCES

1. E. Artin, *Galois theory*, Notre Dame, 1942.

2. E. Artin and G. Whaples, *The theory of simple rings*, Amer. J. Math. vol. 65 (1943) pp. 87–102.

3. H. Cartan, *Théorie de Galois pour les corps non commutatifs*, Ann. École Norm. vol. 64 (1947) pp. 59–77.

4. J. Dieudonné, *Sur le socle d'un anneau et les anneaux simples infinis*, Bull. Soc. Math. France vol. 62 (1942) pp. 46–75.

5. ———, *La théorie de Galois des anneaux simples et semisimples*, Comment. Math. Helv. vol. 21 (1948) pp. 154–184.

6. G. Hochschild, *Automorphisms of simple algebras*, Trans. Amer. Math. Soc. vol. 69 (1950) pp. 292–301.

7. N. Jacobson, *The theory of rings*, Mathematical Surveys, No. 2, New York, 1943.

8. ———, *The radical and semi-simplicity for arbitrary rings*, Amer. J. Math. vol. 67 (1945) pp. 300–320.

9. ———, *A note on division rings*, Amer. J. Math. vol. 64 (1947) pp. 27–36.

10. ———, *On the theory of primitive rings*, Ann. of Math. vol. 48 (1947) pp. 8–21.

11. ———, *Lectures in abstract algebra*, vol. 2, New York, 1953.

12. N. Jacobson and C. E. Rickart, *Jordan homomorphisms of rings*, Trans. Amer. Math. Soc. vol. 69 (1950) pp. 479–502.

13. I. Kaplansky, *Topological representations of algebras*, Trans. Amer. Math. Soc. vol. 68 (1950) pp. 62–75.

14. W. Krull, *Zur Theorie der allgemeinen Zahlringe*, Math. Ann. vol. 99 (1928) pp. 51–70.

15. T. Nakayama, *Galois theory of simple rings*, Trans. Amer. Math. Soc. vol. 73 (1952) pp. 276–292.

16. A. Rosenberg, *Finite-dimensional simple subalgebras of the ring of all continuous linear transformations*, Math. Zeit. vol. 61 (1954) pp. 150–159.

17. B. L. Van der Waerden, *Moderne Algebra*, vol. 2, Berlin, 1940.

18. D. Zelinsky, *Every linear transformation is the sum of nonsingular ones*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 627–630.

NORTHWESTERN UNIVERSITY,
EVANSTON, ILL.