AUTOMORPHISMS OF SIMPLE ALGEBRAS

BY

G. HOCHSCHILD

Introduction. The aim of this paper is to establish a Galois theory for simple (finite-dimensional) algebras. Since the meaning of the designation "Galois theory" has begun to change quite considerably, it may be appropriate to point out that we study the relationships between certain subalgebras of an algebra A on the one hand, and certain groups of automorphisms of A on the other.

The ordinary theory of central simple algebras covers the case of subalgebras containing the center of A. Another special case, in which the subalgebras are subfields of the center, has been discussed from a somewhat different point of view by Teichmueller [7] and by Eilenberg and MacLane [4](1). Some of the recent generalizations of Galois theory to far more general rings—in particular J. Dieudonné's [3]—are concerned chiefly with Galois correspondences between certain subrings of a given ring A on the one hand, and certain rings of endomorphisms on the other. These rings of endomorphisms are intimately related to groups of automorphisms of A in the case of division rings, but in the general case this theory is quite far removed from a theory of automorphisms of A.

The theory given here resembles the Galois theory for division rings as given by H. Cartan [2] and N. Jacobson [6], and covers the special case of division algebras in the same way. Some of our results are related also to those of Dieudonné [3]. However, our method is independent of the new techniques and consists simply in combining the well known results of the theory of simple algebras with those of the ordinary Galois theory for fields, a knowledge of which we shall assume(2).

1. Auxiliary results.

LEMMA 1.1. *Let A be a simple algebra with center C, and let B be a simple subalgebra of A containing C. Let β be an automorphism of B which maps C onto C and denote by $\bar{\beta}$ the automorphism of C which is induced by β. Then β can be extended to an automorphism of A provided only that $\bar{\beta}$ can be so extended.*

Proof. Let σ be an automorphism of A which extends $\bar{\beta}$, that is, which agrees with β on C. Then σ maps B isomorphically onto a simple algebra

Presented to the Society, June 17, 1950; received by the editors November 12, 1949 and, in revised form, December 31, 1949.

(1) Numbers in brackets refer to the bibliography at the end of the paper.

(2) All the results that we require can be found, for instance, in Jacobson [5] and in Artin [1].

$B_1 \supseteq C$. The mapping $\beta\sigma^{-1}$ (defined on B_1) maps B_1 isomorphically onto B and leaves the elements of C fixed. By a standard theorem in the theory of central simple algebras (see, for instance, Theorem 15, p. 101 of [5]) there exists an (inner) automorpism α of A which coincides with $\beta\sigma^{-1}$ on B_1. The mapping $\alpha\sigma$ is an automorphism of A which coincides with β on B.

LEMMA 1.2. *Let K be a simple algebra with center Z, and let G be a finite group of automorphisms of K such that only the identity element of G is an inner automorphism. Let P denote the subfield of Z which consists of the elements fixed under G, and let T be the subring of K which consists of all elements fixed under G. Then T is a simple algebra with center P, and $K = TZ \approx T \times_P Z$, the Kronecker product of T by Z relative to the common subfield P*(3).

Proof. We shall imbed K in a simple algebra A with center P in such a way that the result can be deduced from the theory of commutators in a central simple algebra. The algebra A will be obtained by a construction analogous to that of a crossed product:

As an additive group, A will be the additive group of all mappings of G into K. We make A into a ring by defining, for $\rho, \sigma, \tau \in G$ and $f, g \in A$,

$$(fg)(\tau) = \sum_{\rho\sigma=\tau} f(\rho)\rho\{g(\sigma)\}.$$

Now we imbed K isomorphically in A by the mapping $k \to k^0$ where $k^0(\tau)$ is defined to be equal to k if τ is the identity element of G, and 0 otherwise. If we make the identification $k = k^0$, it is clear that P comes to lie in the center of A, so that we may regard A as an algebra over P. As a (left) space over K, A has a basis of elements u_σ, $\sigma \in G$, where $u_\sigma(\tau)$ is defined to be equal to 1 if $\tau = \sigma$, and 0 otherwise. For $k \in K$ we have then $u_\sigma k = \sigma\{k\} u_\sigma$.

Next we shall prove that A is simple. Let I be any nonzero two-sided ideal in A. We have to show that $I = A$. Let $\sum_{i=1}^r k_i u_{\sigma_i}$, $k_i \in K$, be a nonzero element belonging to I in which the number r of terms is minimal. Then the σ_i are all distinct. Suppose first that $r = 1$, that is, $ku_\sigma \in I$, with $k \neq 0$. Multiplying with k_1 on the left and with $\sigma^{-1}\{k_2\}$ on the right we find that $k_1 k k_2 u_\sigma \in I$, for all $k_1, k_2 \in K$. Since K is simple, we have $KkK = K$, and we may conclude that $u_\sigma \in I$. Hence $1 = u_{\sigma^{-1}} u_\sigma \in I$, so that $I = A$. Hence we may suppose that $r > 1$. Furthermore, the argument we have just made shows that we may assume that $k_r = 1$. Then if we multiply our minimal element by k on the left and subtract from the product the result of multiplying the element by $\sigma_r^{-1}\{k\}$ on the right we find that $\sum_{i=1}^{r-1} (kk_i - k_i\sigma_i\sigma_r^{-1}\{k\}) u_{\sigma_i} \in I$. By the minimality of r and the K-independence of the u_σ this implies that $kk_i = k_i\sigma_i\sigma_r^{-1}\{k\}$, for all $k \in K$ and $i = 1, \cdots, r-1$. This shows that $Kk_i = k_iK$,

(3) If U and V are subrings of a ring A, we shall always denote by UV the subring of A which is generated by U and V. Kronecker products, or direct products, consist of formal sums of formal products, with the requisite identifications.

and hence that Kk_i is a two-sided ideal in K, so that $Kk_i = K$. Hence there is an element $k_i^{-1} \in K$ such that $k_i^{-1}k_i = 1$, and the last equation gives $k_i^{-1}kk_i = \sigma_i\sigma_r^{-1}\{k\}$, which means that $\sigma_i\sigma_r^{-1}$ is an inner automorphism. By assumption on G this gives the contradiction $\sigma_i = \sigma_r$. Hence the case $r > 1$ cannot arise, and we have shown that A is simple.

We claim that the commutator algebra of Z in A coincides with K. In fact, if $f = \sum_{\sigma \in G} f(\sigma)u_\sigma$ commutes with every element $z \in Z$, we obtain, by the independence of the u_σ, $(z - \sigma\{z\})f(\sigma) = 0$. Since Z is a field, we can conclude that if $f(\sigma) \neq 0$ we must have $z = \sigma\{z\}$, for every $z \in Z$, so that σ is inner and therefore the identity automorphism. But this means that $f \in K$, which proves our assertion.

Now let U denote the subring of A which is generated by the u_σ and the field Z. The argument above can be applied to U and shows that U is simple and that the commutator algebra of Z in U coincides with Z. It follows from the second conclusion that the center of U is the fixed subfield (under G) P of Z. Similarly, the center of A must be contained in the commutator algebra K of Z in A and hence must be contained in Z whence we see that it also coincides with P. Further, we have $[U:P] = [U:Z][Z:P] = [Z:P]^2$, because $[U:Z] =$ order of $G = [Z:P]$.

The commutator algebra of U in A must be contained in the commutator algebra K of Z whence we see at once that it coincides with the fixed subring T of K. Hence the commutator algebra of T in A coincides with U(4), and therefore the commutator algebra of T in K is $U \cap K = Z$. Hence the center of T is $T \cap Z = P$. The remaining assertion of Lemma 1.2 now follows directly from a theorem due to Wedderburn and Albert (Theorem 6, p. 51, of Albert's Colloquium Lectures). However, we can obtain our result in a more familiar way: Since T has center P, $T \times_P Z$ is simple(5), and hence the natural homomorphism of $T \times_P Z$ onto TZ is an isomorphism. Hence $[TZ:Z] = [T:P] = [A:P]/[U:P]$, since U is the commutator algebra of T in A(6). But $[A:P] = [Z:P][K:P]$ and $[U:P] = [Z:P]^2$. Hence $[TZ:Z] = [K:P]/[Z:P] = [K:Z]$, and therefore $K = TZ$. This completes the proof.

2. **Galois theory.** Let A be any ring, S an arbitrary subset of A. The group H_S of all automorphisms of A which leaves the elements of S fixed has a certain completeness property: Let us denote by $R(H_S)$ the subring of A which is generated by the set of all those regular elements $a \in A$ which effect inner automorphisms $x \to axa^{-1}$ that belong to H_S. Then H_S must contain every inner automorphism effected by an element of $R(H_S)$. It is evident that only groups with this completeness property can figure in a Galois theory.

(4) See Theorem 19, p. 104, in [5]. We shall use this theorem without further explicit reference from now on.

(5) See Corollary 1, p. 99, in [5].

(6) For this and the next dimensionality relation for commutator algebras, see reference in footnote 4.

This motivates the following definition:

DEFINITION 2.1. A group H of automorphisms of a ring A is called complete if it contains every inner automorphism effected by an element of the subring $R(H)$ of A.

Simple examples show that we must restrict the groups further. Thus, let F_2 denote the algebra of all 2 by 2 matrices with coefficients in an arbitrary field F. Let H be the group of all those inner automorphisms of F_2 which are effected by elements of the form

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}; \qquad ac \neq 0.$$

Then $R(H)$ consists of all matrices of the form

$$\begin{pmatrix} u & 0 \\ v & w \end{pmatrix}.$$

It is easily seen that the subring of F_2 which consists of the elements left fixed by H coincides with F, the center of F_2. But this is left fixed by the larger group of all inner automorphisms of F_2, in violation of a fundamental theorem in the ordinary Galois theory.

The difficulty exhibited here will not arise if we demand that $R(H)$ be a simple ring. Furthermore, we secure a suitable finiteness condition as follows: If H is a group of automorphisms of the simple algebra A with center C, then $R(H)$ is evidently a subalgebra of A containing C. Let H^0 denote the subgroup of H which consists of all the inner automorphisms that belong to H. H^0 is invariant in H. We define the reduced order of H as the product of the order of H/H^0 by the dimension $[R(H):C]$ of $R(H)$ over C. We shall confine our attention to groups of finite reduced order, that is, we shall demand that H/H^0 be a finite group.

DEFINITION 2.2. Let A be a simple algebra with center C. A group H of automorphisms of A is called regular if it is complete, of finite reduced order, and such that $R(H)$ is simple.

The next theorem will show that the relationship between a regular group H of automorphisms of a simple algebra A and the subring $F(H)$ consisting of all the elements of A which are fixed under H is that of the ordinary Galois theory. Furthermore, it will turn out that $F(H)$ is a "regular" subring of A in the sense of the following definition:

DEFINITION 2.3. Let A be a simple algebra with center C. A subring B of A is called almost regular if

(1) B is simple and contains the identity element of A.

(2) C is finite over the subfield $B \cap C$.

(3) BC is simple.

B is called regular if it satisfies (1), (2), and

(4) $B \times_{B \cap C} C$ is simple.

Since there is a natural homomorphism of $B \times_{B \cap C} C$ onto BC, it is clear that (4) implies (3), so that every regular subring is almost regular. Note further that if B is a subalgebra of A, finite over some subfield of C which is contained in B, then (3) implies that B is simple. In fact, if T is the radical of B, then TC is a nilpotent ideal in BC and hence must be (0), whence $T=(0)$, so that B is semi-simple. Hence, if B were not simple, there would be two nonzero two-sided ideals U and V in B such that $UV=(0)$. But then UC and VC would be two-sided nonzero ideals in BC, and thus $UC=BC=VC$, whence $(BC)^2=UCVC=(0)$, contradicting the assumption that BC is simple.

We shall use the following notation: If B is any subalgebra of A over a subfield L of C such that $[C:L]$ is finite, we shall write $[A:B]$ for the positive rational number $[A:L]/[B:L]$. This notation cannot lead to confusion, because the number $[A:L]/[B:L]$ is independent of the particular choice of the field L. We are now in a position to state our theorem.

THEOREM 2.1. *Let A be a simple algebra and let H be a regular group of automorphisms of A. Then the fixed ring $F(H)$ of H in A is regular, and H is the group of all automorphisms of A which leave the elements of $F(H)$ fixed. Furthermore, the reduced order of H is equal to* $[A:F(H)]$.

Proof. Since $R(H)$ is a simple subalgebra of A containing the center C, its commutator algebra, K say, is also a simple algebra containing C, and we have $[K:C][R(H):C]=[A:C]$. Evidently, $F(H) \subseteq K$. Since an automorphism $\sigma \in H$ maps $R(H)$ onto $R(H)$, it must map K onto K. If σ induces an inner automorphism in K, then it leaves the elements of the center Z of K fixed. Since $Z \supseteq C$, σ then leaves the elements of C fixed and hence is an inner automorphism of A, that is, $\sigma \in H^0$. But then σ is effected by an element of $R(H)$ and hence induces the identity automorphism in K. It follows that the restriction of H to K is isomorphic with H/H^0, and hence is finite. We can therefore apply Lemma 1.2 to conclude that $F(H)$ is a simple algebra whose center coincides with the subfield P of Z which consists of the elements fixed under H, and that $K=F(H)Z \approx F(H) \times_P Z$. Clearly, $P=F(H) \cap Z \supseteq F(H) \cap C=F$, say. Also $PC \subseteq Z$, and H maps PC onto PC. F is the subfield of C which consists of the elements fixed under H, and $P=PF$ is the subfield of PC which consists of the elements fixed under H. Since the restriction of H to PC is also isomorphic with H/H^0, we obtain $[PC:P]=$ order of $H/H^0=[Z:P]$, so that $PC=Z$. Similarly we have $[C:F]=[Z:P]$, whence $[Z:F]=[Z:P][P:F]=[(P \times_F C):F]$. Hence the natural homomorphism of $P \times_F C$ onto $PC=Z$ is an isomorphism. In particular, this shows that $P \times_F C$ is simple, and since $F(H)$ has center P, it follows that $F(H) \times_F C$ is simple, that is, that $F(H)$ is a regular subring of A.

The reduced order of H is equal to (order of H/H^0) $[R(H):C]=[C:F]$

$\cdot [A:C]/[K:C]=[A:F]/[K:C]$. Since $K\approx F(H)\times_P Z$, we have $[K:Z]=[F(H):P]$, and hence $[K:C]=[K:Z][Z:C]=[F(H):P][P:F]=[F(H):F]$. Substituting this in the above, we obtain the result that the reduced order of H is equal to $[A:F(H)]$.

Finally, let H_1 denote the group of all automorphisms of A which leave the elements of $F(H)$ fixed. Then $H_1\supseteq H$ and $F(H_1)=F(H)$. Hence $R(H_1)$ is contained in the commutator algebra L of $F(H)$ in A. But evidently L is also the commutator algebra of $F(H)C$, and since $F(H)C$ is simple, it follows that L is also simple. Hence L is generated by its regular elements (to prove this, it suffices to consider the case of a full matrix algebra over a field, which is easily settled). This implies that $L\subseteq R(H_1)$, and hence that $L=R(H_1)$. Now H_1/H_1^0 is still isomorphic with the Galois group of C over F, and in particular is of the same order as H/H^0. Thus H_1 is a regular group, and if we apply the above to H_1 we conclude that the reduced order of H_1 is equal to the reduced order of H, which gives $[R(H_1):C]=[R(H):C]$. Since $R(H_1)\supseteq R(H)$, it now follows that $R(H_1)=R(H)$, and hence that $H_1^0=H^0$. Since H_1/H^0 is of the same order as its subgroup H/H^0, we must have $H_1=H$, which completes the proof.

THEOREM 2.2. *Let A be a simple algebra with center C, and let B be an almost regular subring of A. Then the group H_B of all automorphisms of A which leave the elements of B fixed is regular. If F is the subfield of C which consists of the elements fixed under H_B, then the fixed subring $F(H_B)$ of H_B in A coincides with BF.*

Proof. The argument we made in the last proof, when we showed that $R(H_1)$ was simple, proves here that $R(H_B)$ is simple. Evidently, H_B is complete and H_B/H_B^0 is isomorphic with the Galois group of C over F. Since $F\supseteq B\cap C$, $[C:F]$ is finite, and hence H_B/H_B^0 is finite, and H_B is regular. Since $R(H_B)$ is the commutator algebra of the simple BC (cf. above), BC is the commutator algebra of $R(H_B)$. Hence we have $BF\subseteq F(H_B)\subseteq BC$. Let P denote the center of B. Since BC is simple, its center is a field which evidently contains PC. Hence PC is a field, and we have $BC\approx B\times_P PC$. From this it is easily seen that the fixed ring of H_B in BC is $BS\approx B\times_P S$, where S is the fixed field of H_B in PC. But, clearly, $S=PF$, so that $BS=BF$. On the other hand, since $F(H_B)\subseteq BC$, the fixed ring of H_B in BC coincides with $F(H_B)$. Hence $F(H_B)=BF$, and our proof is complete.

As in the ordinary Galois theory we shall say that A is normal over B if $F(H_B)=B$.

THEOREM 2.3. *Let A be a simple algebra, and suppose that A is normal over a regular subring L. Let B be an almost regular subring of A such that $L\subseteq B$. Then A is normal over B, and B is regular.*

Proof. We have $L\cap C\subseteq B\cap C\subseteq C$, where C is the center of A. Since A is

normal over L, $L\cap C$ is the fixed field of H_L in C. Hence C is normal over $L\cap C$ and therefore also normal over $B\cap C$. Let P denote the center of B. We know from the proof of the last theorem that PC is a field and that $BC\approx B\times_P PC$. Since C is normal over $P\cap C=B\cap C$, PC is normal over P and the automorphisms of PC relative to P induce all the automorphisms of C relative to $P\cap C$. In other words, every automorphism of C which leaves the elements of $P\cap C$ fixed can be extended to an automorphism of PC which leaves the elements of P fixed. Since $BC\approx B\times_P PC$, it follows that every such automorphism can be extended to an automorphism of BC which leaves the elements of B fixed. Since every such automorphism of C is induced by an element of H_L, it follows from Lemma 1.1 that the corresponding automorphism of BC can be extended to an automorphism of A which—of course—is an element of H_B. Hence $P\cap C$ is precisely the fixed field of H_B in C. By Theorem 2.2, we have therefore

$$F(H_B) = B(P \cap C) = B,$$

that is, A is normal over B, and H_B is regular. By Theorem 2.1, $B=F(H_B)$ is regular.

In order to show that Theorem 2.3 does not hold when the condition that BC be simple is omitted, we cite an example given by Teichmueller in [7]:

Let L be a field, and let C be a normal extension field of L with a cyclic Galois group of order greater than 2. Let A be the algebra C_2 of all 2 by 2 matrices with coefficients in C. Let γ be a generator for the Galois group of C over L, and take B to be the ring of all matrices of the form

$$\begin{pmatrix} c & 0 \\ 0 & \gamma\{c\} \end{pmatrix}; \qquad c \in C.$$

We can extend the autmorphisms γ^k to automorphisms of A by defining $\gamma^k\{(c_{ij})\} = (\gamma^k\{c_{ij}\})$. It follows easily that A is normal over L, and evidently L is a regular subring of A. The subring B is simple, but BC is the ring of all matrices of the form

$$\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix},$$

and thus is not simple. The automorphisms of A which carry BC into BC are easily seen to be products of γ^k and inner automorphisms effected by elements of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ or } \begin{pmatrix} 0 & d \\ c & 0 \end{pmatrix}.$$

Since the order of γ is greater than 2, it follows by an easy computation that

an automorphism which leaves the elements of B fixed must be an inner automorphism effected by an element of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

From this it follows at once that $F(H_B)=BC$, which shows that A is not normal over B.

THEOREM 2.4. *Let A be normal over the regular subring L. Let B be a ring such that $L\subseteq B\subseteq A$, and suppose that ϕ is an isomorphism of B into A which leaves the elements of L fixed. Then, if BC and $\phi\{B\}C$ are both simple, ϕ is induced by an element of H_L.*

Proof. Let P denote the center of B. Our conditions imply that B and $\phi\{B\}$ are almost regular, so that PC and $\phi\{P\}C$ are fields. Consider the tower of fields $L\cap C\subseteq P\cap C\subseteq C\subseteq\phi\{P\}C$. Since C is normal over $L\cap C$, and since ϕ maps $P\cap C$ into $\phi\{P\}C$, it follows that $\phi\{P\cap C\}\subseteq C$. The isomorphism $\bar{\phi}$ of $P\cap C$ into C which is induced by ϕ can be extended to an automorphism ϕ^* of C which leaves the elements of $L\cap C$ fixed. From Theorem 2.3 we know that B and $\phi\{B\}$ are regular, so that $BC\approx B\times_{P\cap C}C$ and $\phi\{B\}C\approx\phi\{B\}\times_{\phi\{P\}\cap C}C$. But $\phi\{P\}\cap C=\phi\{P\cap C\}$[7], so that $\phi\{B\}C\approx\phi\{B\}\times_{\phi\{P\cap C\}}C$. Now it is clear that there exists an isomorphism ϕ_1 of $B\times_{P\cap C}C$ onto $\phi\{B\}\times_{\phi\{P\cap C\}}C$ such that $\phi_1\{b\times c\}=\phi\{b\}\times\phi^*\{c\}$. To this there corresponds an isomorphism ϕ_2 of BC onto $\phi\{B\}C$ which coincides with ϕ on B and with ϕ^* on C. Since ϕ^* is induced by an element of H_L, it follows from Lemma 1.1 that ϕ_2 is also induced by an element of H_L. This completes the proof.

The example we have cited above shows also that the condition that BC and $\phi\{B\}C$ be simple cannot be omitted in Theorem 2.4. In fact, the ring B of Teichmueller's example is evidently isomorphic with the center C of A, by an isomorphism which leaves the elements of L fixed. But since every automorphism of A must map C onto C, no isomorphism between B and C is extensible to an automorphism of A.

If H is a group of automorphisms of A, and if B is a subring of A, we shall denote by $H(B)$ the subgroup of H consisting of the elements which map B into B.

Now let A be a simple algebra, and suppose that A is normal over a regular subring L. Let B be a regular subring of A which contains L. If $F(H_L(B))=L$, it follows almost immediately that B is normal over L, and that the group of all automorphisms of B which leave the elements of L fixed is isomorphic with $H_L(B)/H_B$. However, one can give examples to show that L

(7) The inclusion $\phi(P)\cap C\subseteq\phi(P\cap C)$ is proved by proceeding with ϕ^{-1} as we did with ϕ in the beginning of this proof.

need not be regular in B, and that the group of automorphisms of B relative to L need not be regular.

Conversely, if B is normal over L, then it follows from Theorem 2.4 that $F(H_L(B))=L$.

Under suitable regularity conditions, we can obtain a stronger result. This will follow from the next lemma.

LEMMA 2.1. *Let A be a simple algebra with center C, and let B be an almost regular subring of A. Let L be a subring of B containing the identity of A, and such that LPC is simple where P is the center of B. Then $R(H_L(B))$ is simple.*

Proof. Let K be the commutator algebra of LPC in BC. Since LPC is a simple algebra containing the center PC of the simple algebra BC, K is a simple algebra over PC. Also the ring $R(H_B)$ is the commutator algebra of BC in A, and hence is simple and has center PC. We may form the Kronecker product $R(H_B)\times_{PC}K$ which is a simple algebra over PC. It follows that $R(H_B)K\approx R(H_B)\times_{PC}K$, and hence is simple. Write $M=R(H_B)K$.

Clearly, $R(H_L(B))\supseteq M$. Since $R(H_L(B))$ has a finite basis over C which consists of regular elements, we can find a finite set of regular elements $u_1, \cdots, u_m$ such that $R(H_L(B))=Mu_1+\cdots+Mu_m$, and if we take such a set for which m is minimal, we shall have $u_iu_j^{-1}\notin M$ when $i\neq j$. Clearly, $u_iR(H_B)u_i^{-1}\subseteq R(H_B)$ and $u_iKu_i^{-1}\subseteq K$, whence $u_iMu_i^{-1}\subseteq M$. These facts enable us to proceed as in the proof of Lemma 1.2 in order to show that $R(H_L(B))$ is simple: In fact, if I is any two-sided ideal not equal to (0), we take an element in I in which the coefficients of the u_i are not all equal to zero and in which the number of nonzero coefficients is minimal. We may suppose that $\sum_{i=1}^r z_iu_i$, $0\neq z_i\in M$, is such an element. Then we see as in the proof of Lemma 1.2 that we may arrange to have $z_r=1$. If we had $r>1$, we would find as before that the z_i have inverses z_i^{-1}, and that $z=z_iu_iu_r^{-1}zu_ru_i^{-1}z_i^{-1}$, for all $z\in M$. This means that the elements $z_iu_iu_r^{-1}$ commute with every element of M. It follows from this that $z_iu_iu_r^{-1}$ must belong to the commutator algebra BC of $R(H_B)$, and hence also to the commutator algebra LPC of K in BC. On the other hand, $z_iu_iu_r^{-1}$ evidently commutes with every element of L. It follows that $z_iu_iu_r^{-1}\in K$, and hence $u_iu_r^{-1}\in M$, contrary to assumption. Hence we must have $r=1$, which gives $I=A$, and we have proved that $R(H_L(B))$ is simple.

THEOREM 2.5. *Let A be a simple algebra with center C, normal over a regular subring L. Let B be a regular subring of A containing L and with center P. Suppose that LPC is simple. Then B is normal over L if and only if the smallest complete group containing $H_L(B)$ coincides with H_L.*

Proof. If the condition is satisfied, then we obtain easily that $F(H_L(B))=F(H_L)=L$, which implies that B is normal over L.

If G is the smallest complete group containing $H_L(B)$, then we have

$R(G)=R(H_L(B))$, and it follows at once from Lemma 2.1 that G is regular. Now if B is normal over L, we have $F(H_L(B))=L$, and hence $F(G)=L$. Since G is regular, Theorem 2.1 now gives $G=H_L$.

Bibliography

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

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

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

4. S. Eilenberg and S. MacLane, *Cohomology and Galois theory*. I, Trans. Amer. Math. Soc. vol. 64 (1948) pp. 1–20.

5. N. Jacobson, *The theory of rings*, Mathematical Surveys, New York, American Mathematical Society, 1943.

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

7. O. Teichmüller, *Ueber die sogenannte nichtkommutative Galoissche Theorie und die Relation*, Deutsche Mathematik vol. 5 (1940) pp. 138–149.

University of Illinois,
Urbana, Ill.