ON AUTOMORPHISMS AND DERIVATIONS OF SIMPLE RINGS WITH MINIMUM CONDITION([1])

BY

ANDRZEJ BIALYNICKI-BIRULA

I. **Introduction.** Let A, B_1, B_2, C be fields such that $C \subset B_1 \subset A$ and $C \subset B_2 \subset A$, and suppose that A is a finite and normal extension of C. Then it is known that the following conditions are equivalent:

(1) If ϕ_i is an isomorphism of B_i into A leaving the elements of C fixed, $i = 1, 2$, and $\phi_1 | B_1 \cap B_2 = \phi_2 | B_1 \cap B_2$ then there exists an automorphism of A which is a common extension of ϕ_1 and ϕ_2.

(2) B_1 and B_2 are linearly disjoint over $B_1 \cap B_2$.

(2′) $(B_1, B_2) \approx B_1 \otimes_{B_1 \cap B_2} B_2$.

(2″) $[(B_1, B_2) : B_1 \cap B_2] = [B_1 : B_1 \cap B_2] \cdot [B_2 : B_1 \cap B_2]$.

Moreover, if B_1 and B_2 are normal extensions of C then the above conditions are satisfied.

The main purpose of this paper is to give some theorems of this type for division rings and simple rings with minimum condition. First we consider the case where A, B_1, B_2, C are simple rings with minimum condition, A is a Galois([2]) extension of C, B_1 and B_2 are regular subrings([3]) of A containing C, and the center $Z(A)$ of A is infinite. Then we prove (Theorem 1) that if (1) is satisfied then

(3) the centralizer of $B_1 \cap B_2$ in A is equal either to the centralizer of B_1, or to the centralizer of B_2.

Moreover, if B_1 and B_2 are normal extensions of C then (1) is equivalent to (3) (Theorem 2), and $A = (B_1, B_2)$ and (1) imply (2″) (Corollary 3).

Next we consider the case where A, B_1, B_2, C are division rings, A is a finite and normal extension of C, B_1 and B_2 are two division rings between C and A and the center of A is infinite. Then we prove (Theorem 3) that (1) is equivalent to the conjunction of (2) and (3). As a consequence, we obtain that if B_1 and B_2 are normal over C and $A = (B_1, B_2)$ then (1) implies (2′), where the sign $\approx$ occurring in condition (2′) is interpreted as an isomorphism of double $(B_1; B_2)$-modules.

In the next part we consider the analogous question for derivations.

Finally, in the last part, we prove the following theorem([4]): Let A, B, C

([2]) See p. 471 for definition.

([3]) See p. 471 for definition.

([4]) For analogous result for division rings (without assumption that A is a finite extension of C) see Theorem 1 p. 186 in [12].

be simple rings with minimum condition, let C be a regular subring of A, and let B be between C and A. Moreover, suppose that the center of A is infinite. If B is carried into itself by every inner automorphism belonging to $G(A/C)$[5] then either B contains the centralizer of C in A or every inner automorphism belonging to $G(A/C)$ leaves the elements of B fixed. As a consequence of this result, we obtain a characterization of A-normal[6] extensions of C.

In conclusion, the author would like to express his warmest thanks to Professor Gerhard P. Hochschild for his advice and encouragement in the preparation of this paper.

2. Throughout this paper, P, R will denote rings with an identity element. By a subring of a ring with an identity element we mean a subring that contains this identity element.

Let C be a simple subring of R with minimum condition. Then we shall often consider R as a left C-module. It is known[7] that this C-module is free and has a well defined dimension over C. The dimension will be denoted by $[R: C]$. We shall say that R is a finite extension of C if this C-module is finite dimensional, i.e., if $[R: C] < \infty$.

If $a \in R$ then a_r denotes the mapping of R into R defined by the equation $a_r(x) = xa$, for every $x \in R$. If S is a subset of R then S_r denotes the set of all mappings a_r, for $a \in S$. Similarly, a_l denotes the mapping defined by $a_l(x) = ax$, for every $x \in R$, and S_l, where $S \subset R$, denotes the set of all mappings a_l, where $a \in S$. If S_1 and S_2 are two subsets of R then $S_1 \cdot S_2$ denotes the set of all elements of the form $s_1 \cdot s_2$, where $s_i \in S_i$, for $i = 1$, 2, and $(S_1, S_2$ denotes the subring of R generated by $S_1 \cup S_2)$.

R^* denotes the set of all units of R. $Z(R, C)$ denotes the centralizer of C in R. The center of R will be denoted by $Z(R)$. If a is a unit of R then I_a denotes the automorphism of R defined by the equation $I_a(x) = axa^{-1}$, for every $x \in R$. $G(R/C)$ denotes the group of all automorphisms of R leaving the elements of C fixed. Let G_1 be a subgroup of $G(R/C)$. Then R^{G_1} denotes the set of all elements $a \in R$ such that, for every $\phi \in G_1$, $\phi(a) = a$. G_1^0 denotes the subgroup of G_1 consisting of all inner automorphisms belonging to G_1. $R(G_1)$ denotes the subring of R generated by the invertible elements $a \in R$ such that $I_a \in G_1$. We say that G_1 is complete if, for every invertible element $a \in R(G_1)$, $I_a \in G_1$. R is called a normal extension of C if $C = R^{G(A/C)}$.

In the sequel, letters A, B_1, B_2, C, D will denote simple rings with minimum condition.

(i) Let C be a subring of A. Let $\sigma_1, \cdots, \sigma_n$ be elements of $G(A/C)$ such that $G(A/C)^0 \sigma_s \neq G(A/C)^0 \sigma_t$, when $s \neq t$, and let $z_1, \cdots, z_m$ be elements of A that are linearly independent over $Z(A)$. Then $(z_1)_l \sigma_1, \cdots, (z_i)_l \sigma_j, \cdots, (z_m)_l \sigma_n$ are linearly independent over A_r.

[5] See definition below.

[6] See p. 471 for definition.

[7] See e.g. p. 53 in [3].

Proof. Suppose that $(z_1)_l\sigma_1, \cdots, (z_i)_l\sigma_j, \cdots, (z_m)_l\sigma_n$ are linearly dependent over A_r. Let $k+1$ be the minimal number of nonzero coefficients in the nontrivial A_r-linear relations among the $(z_i)_l\sigma_j$. Then there exist $a_{ij} \in A$, $i = 1, \cdots, m$, $j = 1, \cdots, n$, such that $\sum_{i=1}^{m}\sum_{j=1}^{n} (a_{ij})_r(z_i)_l\sigma_j = 0$, where $a_{ij} = 0$ for all but $k+1$ pairs (i, j). We may assume that $a_{11} \neq 0$. Since A is a simple ring, the two-sided ideal $Aa_{11}A$ coincides with A and there are elements x_p, y_p, $p = 1, \cdots, q$, x_p, $y_p \in A$ such that $\sum_{p=1}^{q} x_p a_{11} y_p = 1$, whence $\sum_{p=1}^{q} (y_p)_r(a_{11})_r(x_p)_r = 1_r$. Multiplying the relation $\sum_{i,j}(a_{ij})_r(z_i)_l\sigma_j = 0$ by $(y_p)_r$ from the left and by $(\sigma_1^{-1}(x_p))_r$ from the right and summing for $p = 1, \cdots, q$ we obtain the relation $\sum_{i,j}(b_{ij})_r(z_i)_l\sigma_j = 0$, where $b_{ij} \in A$, $b_{11} = 1$ and $b_{ij} \neq 0$ for exactly $k+1$ pairs (i, j). Let $a \in A$. Then we have $\sum_{i,j} a_r(b_{ij})_r(z_i)_l\sigma_j = 0$ and $\sum_{i,j}(b_{ij})_r(z_i)_l\sigma_j(\sigma_1^{-1}(a))_r = 0$, i.e.,

$$\sum_{i,j}(b_{ij})_r(\sigma_j\sigma_1^{-1}(a))_r(z_i)_l\sigma_j = 0.$$

Subtracting this from the previous relation we obtain $\sum_{i,j}(c_{ij})_r(z_i)_l\sigma_j = 0$, where $c_{ij} = b_{ij}a - \sigma_j\sigma_1^{-1}(a)b_{ij}$ and the number of pairs (i, j) for which $c_{ij} \neq 0$ is less than $k+1$ since $c_{11} = 0$. Hence, we obtain, by the minimality of $k+1$, that $c_{ij} = 0$, for all $i = 1, \cdots, m$, $j = 1, \cdots, n$. Thus $b_{ij}a - \sigma_j\sigma_1^{-1}(a)b_{ij} = 0$. This shows that $b_{ij}A = Ab_{ij}$, and, since A is simple, we may conclude that each b_{ij} is either 0 or a unit. Therefore, if $b_{ij} \neq 0$ then $\sigma_j\sigma_1^{-1} = I_{b_{ij}}$ and so $j = 1$, since $G(A/C)^0\sigma_s \neq G(A/C)^0\sigma_t$ when $s \neq t$. Hence we may label the z_i so that there are nonzero elements $b_{i1} \in A$, $i = 1, \cdots, k+1$, such that $\sum_{i=1}^{k+1}(b_{i1})_r(z_i)_l\sigma_1 = 0$ and $b_{11} = 1$, i.e., $(z_1)_l + \sum_{i=2}^{k+1}(b_{i1})_r(z_i)_l = 0$. Now let $a \in A^*$. Then $a_r^{-1}(z_1)_l a_r + \sum_{i=2}^{k+1} a_r^{-1}(b_{i1})_r a_r(z_i)_l = 0$ and so $(z_1)_l + \sum_{i=2}^{k+1}(ab_{i1}a^{-1})_r(z_i)_l = 0$. Subtracting the last relation from $(z_1)_l + \sum_{i=2}^{k+1}(b_{i1})_r(z_i)_l = 0$, we obtain

$$\sum_{i=2}^{k+1}(b_{i1} - ab_{i1}a^{-1})_r(z_i)_l = 0.$$

By the minimality of $k+1$, this implies $b_{i1} = ab_{i1}a^{-1}$. Hence $b_{i1} \in Z(A)$, because A^* generates A. Therefore, $(z_1)_l + \sum_{i=2}^{k+1}(b_{i1})_l(z_i)_l = 0$ and so $z_1 + \sum_{i=2}^{k+1} b_{i1}z_i = 0$. This gives a contradiction, because we have supposed that the z_i are linearly independent over $Z(A)$. Thus the theorem is proved[8].

The following is well known[9]:

(ii) Let C be a subring of A and let $[A; C] < \infty$. Let $E(A : C)$ be the ring of all endomorphisms of the C-module A. Then $[E(A; C) : A_r] = [A : C]$.

Combining (i) and (ii) we obtain

(iii) Let C be a subring of A and let $[A : C] < \infty$. Then $[Z(A, C) : Z(A)] \cdot [G(A/C) : G(A/C)^0] \leq [A : C] < \infty$. In particular, $[Z(A, C) : Z(A)] < \infty$.

REMARK. We shall prove later[10] that if a ring R with the identity element

---

[8] The proof is patterned after a proof of a theorem of G. Hochschild.

[9] See e.g. p. 55 in [3].

[10] See Lemma 2.

1 contains an infinite field F such that $[R:F] < \infty$ then every element of R can be represented as a sum of units. Hence it follows from (iii) that if $Z(A)$ is infinite than $Z(A, C) = R(G(A/C))$.

Let C be a subring of A. Then C is called a regular subring of A if C is simple with minimum condition, $[A:C] < \infty$ and $Z(A, C)$ is simple.

A subgroup G_1 of $G(A/C)$ is said to be regular if: (1) G_1 is complete, (2) $[G_1:G_1^0] < \infty$ and (3) $R(G_1)$ is simple and $[R(G_1):Z(A)] < \infty$.

A is called a Galois extension of a subring P if $A^{G(A/P)} = P$ and $G(A/P)$ is regular.

(iv)([11]) If G_1 is a regular group of automorphisms of A then A^{G_1} is a regular subring of A, and $[A:A^{G_1}] = [G_1:G_1^0] \cdot [R(G_1):Z(A)]$. Hence if A is a Galois extension of P then P is a regular subring of A.

REMARK. It follows from (iv) that if $[Z(A, C):Z(A)] \cdot [G(A/C):G(A/C)^0]$ $= [A:C]$ and $G(A/C)$ is regular then $C = A^{G(A/C)}$ and hence is a regular subring of A. One can also prove that if $[A:C] = [Z(A, C):Z(A)]$ $\cdot [G(A/C):G(A/C)^0]$, which is equivalent to the assumption that A is a strongly normal([12]) extension of C, then C is "close" to being regular; namely, $Z(A, C)$ is then a direct sum of mutually isomorphic simple rings.

Let $C \subset B \subset A$ be successive finite extensions of C. If $\phi \in G(A/C)$ then $\phi | B$ denotes the restriction of ϕ to B. If G_1 is a subgroup of $G(A/C)$ then $G_1 | B$ denotes the set of all elements of the form $\phi | B$ where $\phi \in G_1$. Let B be a regular subring of A. Then $G(B, A/C)$ denotes the set of all isomorphisms ϕ of B into A leaving the elements of C fixed and such that $\phi(B)$ is a regular subring of A. It is easy to see that if $\psi \in G(A/C)$ then $\psi | B \in G(B, A/C)$.

B is called an A-normal extension of C if for every $\phi \in G(A/C)$ $\phi(B) = B$.

Let B_1 and B_2 be extensions of C and let A be an extension of B_1 and B_2. If $\phi_1 \in G(B_1, A/C)$, $\phi_2 \in G(B_2, A/C)$ then an element $\phi \in G(A/C)$ is called an extension of the pair (ϕ_1, ϕ_2) if $\phi | B_1 = \phi_1$ and $\phi | B_2 = \phi_2$. The pair (ϕ_1, ϕ_2) is called compatible if $\phi_1 | B_1 \cap B_2 = \phi_2 | B_1 \cap B_2$.

In the sequel we shall use the following theorems:

(v)([13]) FUNDAMENTAL THEOREM OF GALOIS THEORY. *Let A be a Galois extension of C. Let $\mathfrak{A}$ be the collection of all regular subgroups of $G(A/C)$ and let $\mathfrak{B}$ be the collection of all regular subrings of A containing C. Then there exists the usual 1-1 correspondence between $\mathfrak{A}$ and $\mathfrak{B}$. In the direction from $\mathfrak{A}$ to $\mathfrak{B}$, we have $G_1 \to A^{G_1}$; in the other direction, we have $B \to G(A/B)$.*

(vi)([14]) *Let A be a Galois extension of C and let B be a regular subring between C and A. Then every isomorphism $\phi \in G(B, A/C)$ has an extension $\psi \in G(A/C)$.*

([11]) See Theorem 1, p. 282 in [14].
([12]) See p. 277 in [14] for definition.
([13]) See Theorem 5, p. 285, in [14].
([14]) See Theorem 6, p. 285, in [14].

LEMMA 1. *Let A be a Galois extension of C and let B_1, B_2 be regular subrings between C and A. The following three conditions are equivalent:*

(a) $G(A/B_2)\big| B_1 = G(B_1, A/B_1 \cap B_2)$.

(b) *every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$.*

(c) $G(A/B_1 \cap B_2) = G(A/B_2) \cdot G(A/B_1)$.

Proof. (a)$\Rightarrow$(b). Let us take ϕ_1 and ϕ_2 as in (b). It follows from (vi) that there exists $\psi_2 \in G(A/C)$ such that $\psi_2 | B_2 = \phi_2$. Let us put $\gamma = \psi_2^{-1}\phi_1$. Then $\gamma \in G(B_1, A/B_1 \cap B_2)$ and it follows from (a) that there exists $\psi \in G(A/B_2)$ such that $\psi | B_1 = \gamma$. Now $\psi_2\psi | B_1 = \psi_2\psi_2^{-1}\phi_1 | B_1 = \phi_1 | B_1$ and $\psi_2\psi | B_2 = \psi_2 | B_2 = \phi_2$. Hence $\psi_2\psi$ is an extension of (ϕ_1, ϕ_2).

(b)$\Rightarrow$(c). Let $\phi \in G(A/B_1 \cap B_2)$. It follows from (b) that there exists an automorphism $\psi \in G(A/B_1 \cap B_2)$ such that $\psi | B_2 = \phi | B_2$ and $\psi | B_1$ is the identity automorphism of B_1. Now $\phi = (\phi\psi^{-1})\psi$, $\phi\psi^{-1} \in G(A/B_2)$, $\psi \in G(A/B_1)$. Thus $\phi \in G(A/B_2) \cdot G(A/B_1)$.

(c)$\Rightarrow$(a). It follows from (c) that $G(A/B_1 \cap B_2)\big| B_1 = G(A/B_2)G(A/B_1)\big| B_1 = G(A/B_2)\big| B_1$. But by (vi) $G(A/B_1 \cap B_2)\big| B_1 = G(B_1, A/B_1 \cap B_2)$, whence $G(A/B_2)\big| B_1 = G(B_1, A/B_1 \cap B_2)$.

The following corollary is an immediate consequence of the lemma:

COROLLARY 1. *Let A, B_1, B_2, C be as in Lemma 1. If $G(A/B_2)\big| B_1 = G(B_1, A/B_1 \cap B_2)$ then $G(A/B_1)\big| B_2 = G(B_2, A/B_1 \cap B_2)$.*

Let V be a finite dimensional vector space over a field F. If S is a subset of V then $\overline{S}$ denotes the smallest algebraic subset of V containing S.

LEMMA 2. *Let R be a ring with an identity element, let F be an infinite field contained in R and suppose that $[R:F] < \infty$. Let us consider R as a left vector space over F. Then $(R^*)^- = R$.*

Proof. Let d be the function on R defined by $d(a) = \det(a_r)$. Then d is evidently a polynomial function on R, and the elements of R^* are precisely the elements a such that $d(a) \neq 0$. Now let p be a polynomial function vanishing on R^*. Then $dp = 0$. Since $d \neq 0$, this gives $p = 0$. Thus the ideal associated with R^* is the 0-ideal, whence $(R^*)^- = R$.

LEMMA 3. *Let R be a finite dimensional algebra over an infinite field F. Let $\{V_j, W_j\}_{j=1,\ldots,n}$ be a family of pairs of F-vector spaces contained on R. If $R = \bigcup_{j=1}^n (V_j W_j)^-$ then there exists an index j_0, such that either $\dim V_{j_0} > 2^{-1} \dim_F R$ or $\dim W_{j_0} > 2^{-1} \dim_F R$.*

Proof. Let $T_j = (V_j W_j)^-$, $p_j = \dim V_j$, $q_j = \dim W_j$. Then $\dim T_j \leq p_j + q_j - 1$. Indeed, let M_j be a $(p_j - 1)$-dimensional F-vector subspace of V_j, let $a_j \in V_j$, $a_j \notin M_j$ and suppose that $a_j + M_j$ is the set of all elements of the form $a_j + m$, where $m \in M_j$. Then it is easy to see that $V_j \cdot W_j = (a_j + M_j) \cdot W_j \cup M_j \cdot W_j$. Moreover $(a_j + M_j) \times W_j$ and $M_j \times W_j$ are $(p_j - 1 + q_j)$-dimensional

algebraic subsets of $V_j \times W_j$, and the mapping f_j from $V_j \times W_j$ into R defined by the equality $f_j(x, y) = xy$, for every $x \in V_j$, $y \in W_j$, is a polynomial mapping. Hence dim $T_{j_n} \leq p_j + q_j - 1$.

Now let us suppose that $R = \bigcup_{j=1}^{n} (V_j W_j)^- = \bigcup_{j=1}^{n} T_j$. Then there exists an index j_0 such that $T_{j_0} = R$, because R is irreducible. Hence $\dim_F R = \dim T_{j_0} \leq p_{j_0} + q_{j_0} - 1$. Let us suppose that $p_{j_0} \leq q_{j_0}$. Then $\dim_F R \leq 2q_{j_0} - 1 < 2q_{j_0}$, hence $q_{j_0} > 2^{-1} \dim_F R$ and the lemma is proved.

LEMMA 4. *Let R be a finite dimensional algebra with the identity 1 over an infinite field F. Let $\{C_j, D_j\}_{j=1,\dots,n}$, $\{d_j\}_{j=1,\dots,n}$ be a family of pairs of simple rings with minimum condition between F and R, and a subset of R, respectively. If $R^* = \bigcup_{j=1}^{n} C_j^* D_j^* d_j$ then there exists an index j_0, such that either $R = C_{j_0}$ or $R = D_{j_0}$.*

Proof. Let us suppose that $R^* = \bigcup_{j=1}^{n} C_j^* D_j^* d_j$. Then, by Lemma 2, $R = (R^*)^- = \bigcup_{j=1}^{n} (C_j^* D_j^* d_j)^- \subset \bigcup_{j=1}^{n} (C_j D_j d_j)^-$. But C_j and $D_j d_j$ are F-vector subspaces of R. Therefore, it follows from Lemma 3 that there exists an index j_0 such that either $[C_{j_0}:F] = \dim_F C_{j_0} > 2^{-1} \dim_F R = 2^{-1}[R:F]$ or $\dim_F D_{j_0} \cdot d_{j_0} > 2^{-1}[R:F]$. Hence either $[C_{j_0}:F] > 2^{-1}[R:F]$ or $[D_{j_0}:F] > 2^{-1}[R:F]$. But $[R:F]$ is divisible by $[C_{j_0}:F]$ and $[D_{j_0}:F]$. Therefore we get that either $[R:F] = [C_{j_0}:F]$ or $[R:F] = [D_{j_0}:F]$. If $[R:F] = [C_{j_0}:F]$ then $R = C_{j_0}$; if $[R:F] = [D_{j_0}:F]$ then $R = D_{j_0}$. This completes the proof of the lemma.

THEOREM 1. *Let A be a Galois extension of C. Let B_1, B_2 be regular subrings between C and A and suppose that $Z(A)$ is infinite. If every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$ then either $Z(A, B_1 \cap B_2) = Z(A, B_1)$ or $Z(A, B_1 \cap B_2) = Z(A, B_2)$.*

Proof. Let us suppose that every compatible pair (ϕ_1, ϕ_2) where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$. Then it follows from Lemma 1 that $G(A/B_1 \cap B_2) = G(A/B_2) \cdot G(A/B_1)$. Let $\{\phi_1^i, \cdots, \phi_{m_i}^i\}$, $i = 1, 2$, be a set of representatives of the cosets of the subgroup $G(A/B_i)^0$ in $G(A/B_i)$. Then every automorphism $\psi_i \in G(A/B_i)$, $i = 1, 2$, can be represented in the form $I_{c_i} \phi_{j_i}^i$, where $1 \leq j_i \leq m_i$, and $c_i \in Z(A, B_i)^*$. For every j, $1 \leq j \leq m_2$, there exists at most one integer k, $1 \leq k \leq m_2$, such that $\phi_j^2 \phi_k^1$ is an inner automorphism. Indeed, if $\phi_j^2 \phi_{k_1}^1$ and $\phi_j^2 \phi_{k_2}^1$ are inner then also $(\phi_j^2 \phi_{k_1}^1)^{-1} \phi_j^2 \phi_{k_2}^1$ is inner. But $(\phi_j^2 \phi_{k_1}^1)^{-1} \phi_j^2 \phi_{k_2}^1 = (\phi_{k_1}^1)^{-1} \phi_{k_2}^1$, hence $k_1 = k_2$. Therefore we may suppose that the only inner automorphisms of the form $\phi_j^2 \phi_k^1$ are the $\phi_j^2 \phi_j^1$, with $1 \leq j \leq n$. For each such j choose $c_j \in Z(A, B_1 \cap B_2)^*$ such that $\phi_j^2 \phi_j^1 = I_{c_j}$.

Let $a \in Z(A, B_1 \cap B_2)^*$, then I_a can be represented in the form $\phi_2 \phi_1$, where $\phi_i \in G(A/B_i)$, for $i = 1, 2$, and hence in the form $I_b \phi_j^2 I_c \phi_k^1$, where $b \in Z(A, B_2)^*$, $c \in Z(A, B_1)^*$, $1 \leq j \leq m_2$ and $1 \leq k \leq m_1$. Therefore $I_a = I_b I_{\phi_j^2(c)} \phi_j^2 \phi_k^1$ and $\phi_j^2 \phi_k^1$ is inner. Hence we get $j = k$ and $\phi_j^2 \phi_k^1 = I_{c_j}$. Thus every element $a \in Z(A, B_1 \cap B_2)^*$ can be represented in the form bdc_j, where $b \in Z(A, B_2)^*$, $d \in \phi_j^2(Z(A, B_1)^*)$ and $1 \leq j \leq n$. On the other hand, $Z(A, B_2)^*$

$\cdot \phi_j^2(Z(A, B_1)^*) \cdot c_j \subset Z(A, B_1 \cap B_2)^*$, for every $1 \leqq j \leqq n$. Hence $Z(A, B_1 \cap B_2)^*$ $= \bigcup_{j=1}^n Z(A, B_2)^* \cdot \phi_j^2(Z(A, B_1)^*) \cdot c_j$. Now $Z(A, B_1 \cap B_2)$ is a finite extension of the infinite field $Z(A)$ and, for every $\phi \in G(A/B_1 \cap B_2)$ and $i = 1, 2, \phi(Z(A, B_i))$ is a simple ring with minimum condition containing $Z(A)$. Hence it follows from Lemma 4 that either $Z(A, B_1 \cap B_2) = Z(A, B_2)$ or $Z(A, B_1 \cap B_2) = \phi_j^2(Z(A, B_1))$ for some j. Since $\phi_j^2 \in G(A/B_1 \cap B_2)$, the second equality implies that $Z(A, B_1 \cap B_2) = Z(A, B_1)$. Therefore we conclude that either $Z(A, B_1 \cap B_2) = Z(A, B_2)$ or $Z(A, B_1 \cap B_2) = Z(A, B_1)$ and the theorem is proved.

COROLLARY 2. *Let A be a Galois extension of C. Let B_1, B_2 be two regular subrings between C and A and suppose that $Z(A)$ is infinite. If every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$ then either $G(B_1/B_1 \cap B_2)$ or $G(B_2/B_1 \cap B_2)$ contains no nontrivial inner automorphisms.*

Proof. It follows from Theorem 1 that if the assumption of the corollary is satisfied then either $Z(A, B_1 \cap B_2) = Z(A, B_1)$ or $Z(A, B_1 \cap B_2) = Z(A, B_2)$. If $Z(A, B_1 \cap B_2) = Z(A, B_1)$ then $Z(B_1, B_1 \cap B_2) = Z(B_1)$ and therefore $G(B_1/B_1 \cap B_2)^0$ is trivial. Similarly, if $Z(A, B_1 \cap B_2) = Z(A, B_2)$ then $G(B_2/B_1 \cap B_2)^0$ is trivial.

LEMMA 5. *Let $C \subset P \subset B \subset A$ be successive extensions of C such that A is a Galois extension of C, B is a regular subring of A and B is a normal extension of P. If $B \subset A^{G(A/P)^0}$ then P is a regular subring of A, B is an A-normal extension of P, and $G(B/P)$ is finite.*

Proof. Let us suppose that $B \subset A^{G(A/P)^0}$. Then $G(B/P)$ contains no nontrivial inner automorphism. Hence $\text{card}(G(B/P)) = [G(B/C): G(B/C)^0]$. But it follows from (iii) that $[G(B/C): G(B/C)^0] \leqq [B: C]$. Thus $G(B/P)$ is finite, since $[B: C] \leqq [A: C] < \infty$. Hence $G(B/P)$ is regular, and it follows from (iv) that P is a regular subring of B. Since $B \subset A^{G(A/P)^0}$, we have $Z(A, P) = Z(A, B)$, so that $Z(A, P)$ is simple. As a regular subring of B, P is simple with minimum condition. Also $[A: P] \leqq [A: C] < \infty$, and we conclude that P is a regular subring of A.

Now let $D = A^{G(A/P)^0}$. Then D is an A-normal extension of P. Therefore, in order to prove that B is an A-normal extension of P, it suffices to show that B is a D-normal extension of P. D is a regular subring of A because $D = A^{G(A/P)^0}$ $= A^{G(A/B)^0}$ and $G(A/B)^0$ is regular. Moreover D is a Galois extension of P and $[D: P] = \text{card}(G(D/P))$. In fact, we see as above for $G(B/P)$ that $G(D/P)$ is finite and contains no nontrivial inner automorphism, and $D^{G(D/P)}$ $= A^{G(A/P)} = P$. Now D is a Galois extension of B and $[D: B] = \text{card}(G(D/B))$, because B is a regular subring of D (B is a simple ring with minimum condition, $[D: B] \leqq [A: B] < \infty$ and $Z(D, B) = Z(D)$). Next, B is a Galois extension of P, since B is a normal extension of P and $G(B/P)$ is finite and contains

no nontrivial inner automorphism. Therefore $[B:P] = \mathrm{card}(G(B/P))$. By (vi), every element of $G(B/P)$ is the restriction to B of an element of $G(D/P)$. Choose elements $\psi_1, \cdots, \psi_{[B:P]}$ in $G(D/P)$ whose restrictions to B make up the group $G(B/P)$. Then the cosets $\psi_i G(D/B)$ are distinct, so that $\bigcup_{i=1}^{[B:P]} \psi_i G(D/B)$ consists of $[D:B] \cdot [B:P] = [D:P]$ elements of $G(D/P)$. Hence $G(D/P) = \bigcup_{i=1}^{[B:P]} \psi_i G(D/B)$. If $\phi \in G(D/B)$ then $\psi_i \phi(B) = \psi_i(B) = B$. Hence $\psi(B) = B$, for every $\psi \in G(D/P)$, i.e., B is a D-normal extension of P. This completes the proof of Lemma 5.

THEOREM 2. *Let A be a Galois extension of C, and let B_1, B_2 be regular subrings between C and A. Moreover, let us suppose that B_1 and B_2 are normal extensions of $B_1 \cap B_2$, and $Z(A)$ is infinite.*

I. *The following two conditions are equivalent, for $i = 1, 2$.*

(a_i) *B_i is an A-normal extension of $B_1 \cap B_2$ and $G(B_i/B_1 \cap B_2)$ contains no nontrivial inner automorphism.*

(b_i) *$Z(A, B_1 \cap B_2) = Z(A, B_i)$.*

Moreover, if one of the conditions is satisfied then $B_1 \cap B_2$ is a regular subring of A, and $G(B_i/B_1 \cap B_2)$ is finite.

II. *The following three conditions are equivalent:*

(a) *(a_1) or (a_2),*

(b) *(b_1) or (b_2),*

(c) *every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$.*

Proof. I. (b_i)$\Rightarrow$(a_i). If $Z(A, B_1 \cap B_2) = Z(A, B_i)$ then $G(B_i/B_1 \cap B_2)$ contains no nontrivial inner automorphism and $B_i \subset A^{G(A/B_1 \cap B_2)^0}$. Hence it follows from Lemma 5 that B_i is an A-normal extension of $B_1 \cap B_2$, $B_1 \cap B_2$ is a regular subring of A and $G(B_i/B_1 \cap B_2)$ is finite.

(a_i)$\Rightarrow$(b_i). Let h be the map from $G(A/B_1 \cap B_2)$ into $G(B_i/B_1 \cap B_2)$ defined by $h(\psi) = \psi | B_i$, for every $\psi \in G(A/B_1 \cap B_2)$. Then h is a homomorphism. $G(B_i/B_1 \cap B_2)$ contains no nontrivial inner automorphism. Hence, it follows from (iii) that, $\mathrm{card}(G(B_i/B_1 \cap B_2)) \leqq [G(B_i/C) : G(B_i/C)^0] \leqq [B_i : C] < \infty$. Therefore $h(G(A/B_1 \cap B_2)^0)$ is also finite. But $h(G(A/B_1 \cap B_2)^0) \approx Z(A, B_1 \cap B_2)^*/Z(A, B_i)^*$. Hence there exists a finite set $\{d_1, \cdots, d_n\} \subset Z(A, B_1 \cap B_2)$ such that $Z(A, B_1 \cap B_2)^* = \bigcup_{j=1}^n Z(A, B_i)^* d_j$. $Z(A, B_i)$ is a simple ring with minimum condition and $[Z(A, B_1 \cap B_2) : Z(A)] < \infty$. Hence the assumptions of Lemma 4 are satisfied for $C_j = D_j = Z(A, B_i)$, $F = Z(A)$, $R = Z(A, B_1 \cap B_2)$. Thus $Z(A, B_1 \cap B_2) = Z(A, B_i)$.

II. The implications (b)$\Rightarrow$(a) and (c)$\Rightarrow$(b) follow from the first part of this theorem and Theorem 1, respectively. Hence it remains to prove that (a_i) implies (c) for $i = 1, 2$.

Let us suppose that (a_1) holds. Then $G(B_1, A/B_1 \cap B_2) = G(B_1/B_1 \cap B_2)$, since B_1 is an A-normal extension of $B_1 \cap B_2$. Now $G(A/B_2) | B_1$ is a complete subgroup of $G(B_1/B_1 \cap B_2)$, because $G(B_1/B_1 \cap B_2)$ does not contain any non-

trivial inner automorphism. Hence $G(A/B_2)|B_1$ is a regular subgroup of $G(B_1/B_1 \cap B_2)$, since it follows from the first part of the theorem that $G(B_1/B_1 \cap B_2)$ is finite. Moreover $B_1^{G(A/B_2)|B_1} = A^{G(A/B_2)} \cap B_1 = B_2 \cap B_1$. Hence it follows from (v) that $G(A/B_2)|B_1 = G(B_1/B_1 \cap B_2)$. Therefore $G(A/B_2)|B_1 = G(B_1, A/B_1 \cap B_2)$ and hence, by Lemma 1, we obtain (c). Similarly, we prove that (a_2) implies (c). Thus (a) implies (c) and this completes the proof of Theorem 2.

COROLLARY 3. *Let A be a Galois extension of C and let B_1, B_2 be regular subrings between C and A. Moreover, let us suppose that B_1, B_2 are normal extensions of $B_1 \cap B_2$, $Z(A)$ is infinite, and $A = (B_1, B_2)$.*

If every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$ then $B_1 \cap B_2$ is a regular subring of A $[A : B_1 \cap B_2]$ $= [A : B_1][A : B_2]$, $[A : B_1] = [B_2 : B_1 \cap B_2]$ and $[A : B_2] = [B_1 : B_1 \cap B_2]$.

Proof. Let us suppose that every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$. Then it follows from Theorem 2 that, either for $i = 1$ or else for $i = 2$, $Z(A, B_1 \cap B_2) = Z(A, B_i)$, B_i is an A-normal extension of $B_1 \cap B_2$ and $G(B_i/B_1 \cap B_2)$ is finite and does not contain any nontrivial inner automorphism. Let us suppose that this holds for $i = 1$. Then $G(A/B_2)$ contains no nontrivial inner automorphism. Indeed $Z(A, B_2) \subset Z(A, B_1 \cap B_2) = Z(A, B_1)$, and so $Z(A, B_2) \subset Z(A, B_1) \cap Z(A, B_2)$ $= Z(A, (B_1, B_2)) = Z(A, A) = Z(A)$. Let h be the homomorphism of $G(A/B_2)$ into $G(B_1/B_1 \cap B_2)$ defined by $h(\psi) = \psi|B_1$, for every $\psi \in G(A/B_2)$ (B_1 is an A-normal extension of $B_1 \cap B_2$; hence $\psi|B_1 \in G(B_1/B_1 \cap B_2)$ for every $\psi \in G(A/B_2)$). Then $h(G(A/B_2))$ is a regular subgroup of $G(B_1/B_1 \cap B_2)$, because $G(B_1/B_1 \cap B_2)$ is finite and does not contain any nontrivial inner automorphism. Moreover $B_1^{h(G(A/B_2))} = B_1^{G(A/B_2)|B_1} = A^{G(A/B_2)} \cap B_1 = B_1 \cap B_2$. Hence $h(G(A/B_2)) = G(B_1/B_1 \cap B_2)$. But h is a monomorphism, since $A = (B_1, B_2)$. Therefore, h maps $G(A/B_2)$ isomorphically onto $G(B_1/B_1 \cap B_2)$ and $\mathrm{card}(G(A/B_2)) = \mathrm{card}(G(B_1/B_1 \cap B_2))$. By Theorem 2, $B_1 \cap B_2$ is regular in A. Hence $[A : B_1 \cap B_2]$, $[B_1 : B_1 \cap B_2]$ and $[B_2 : B_1 \cap B_2]$ are well defined and finite. Moreover, $[A : B_2] = \mathrm{card}(G(A/B_2)) = \mathrm{card}(G(B_1/B_1 \cap B_2)) = [B_1 : B_1 \cap B_2]$. But $[A : B_1 \cap B_2] = [A : B_1] \cdot [B_1 : B_1 \cap B_2] = [A : B_2][B_2 : B_1 \cap B_2]$. Hence $[A : B_1 \cap B_2] = [A : B_1][A : B_2]$, $[A : B_1] = [B_2 : B_1 \cap B_2]$ and $[A : B_2] = [B_1 : B_1 \cap B_2]$.

3. In the sequel, letters F, K, L, M, N will denote division rings. If F is a division subring of K then the set of all F-linear endomorphisms of K will be denoted by $E(K; F)$.

Let $F \subset N \subset K$ be successive extensions of F. Then $E(N, K; F)$ denotes the set of all F-linear mappings of N into K. It is easy to see that $G(N, K/F) \subset E(N, K; F)$. If $f \in E(N, K; F)$, $a \in N$ and $b \in K$ then $f \cdot a_r \in E(N, K; F)$ and $b_r \cdot f \in E(N, K; F)$. Hence $E(N, K; F)$ can be considered as a $(K; N)$-module.

The following easy result is recorded here for reference:

(vii) Let K be a finite extension of F. Then

(a) F is a regular subring of K,

(b) a subgroup G_1 of $G(K/F)$ is regular if and only if G_1 is complete. In particular $G(K/F)$ is regular.

(c) K is a Galois extension of F if and only if K is a normal extension of F.

The following theorem follows from (vi) and (vii):

(viii)[15] Let K be a finite and normal extension of F and let N be an extension of F such that $N \subset K$. Every isomorphism $\phi \in G(N, K/F)$ has an extension $\psi \in G(K/F)$.

Let N_1, N_2 be two extensions of F and let K be an extension of N_1 and N_2. We shall say that N_1 is linearly disjoint from N_2 if every subset of N_1 that is left linearly independent over $N_1 \cap N_2$ is also left linearly independent over N_2. If N_1 is linearly disjoint from N_2, and N_2 is linearly disjoint from N_1, then we say that N_1, N_2 are linearly disjoint.

We shall use the following theorems.

(ix)[16] Let K be a normal and finite extension of F. Then

$$(K_r, G(K/F)) = E(K; F).$$

(x) Let K be a normal and finite extension of F and let N be a subring of K containing F. If $\phi, \psi_1, \cdots, \psi_n \in G(N, K/F)$ and $\phi = \sum_{i=1}^{n} a_r^i \psi_i$, where $a^i \in K$, then there exist j, $(1 \leq j \leq n)$, and an element $a \in Z(K, F)$ such that $\phi = I_{a^{-1}} \psi_j$.

The following proof of (x) is contained in the proof of Theorem 1 [12, p. 162]:

It is easy to see that if $\psi \in G(N, K/F)$ then $K_r \cdot \psi$ is a simple $(K; N)$-module; hence $K_r \psi_1 + \cdots + K_r \psi_n$ is a completely reducible $(K; N)$-module and $K_r \phi \subset K_r \psi_1 + \cdots + K_r \psi_n$ implies that there exists j, $1 \leq j \leq n$, such that $K_r \phi$ is $(K; N)$-isomorphic to $K_r \psi_j$. Let us suppose that h is a $(K; N)$-isomorphism of $K_r \phi$ onto $K_r \psi_j$ and let $h(\phi) = a_r \psi_j$ where $a \in K$. Then for any $x \in N$ we have

$$a_r \psi_j(x)_r \psi_j = a_r \psi_j x_r = h(\phi) x_r = h(\phi x_r) = h(\phi(x)_r \cdot \phi) = \phi(x)_r h(\phi) = \phi(x)_r a_r \psi_j$$

and therefore $\psi_j(x)a = a\phi(x)$. Thus $\phi = a_1^{-1} a_r \psi_j = I_{a^{-1}} \psi_j$.

LEMMA 6. *Let K be a finite and normal extension of F and let N_1, N_2 be two division rings between F and K. If $G(K/N_2) \mid N_1 = G(N_1, K/N_1 \cap N_2)$ then N_1, N_2 are linearly disjoint.*

Proof. Let us suppose that $G(K/N_2) \mid N_1 = G(N_1, K/N_1 \cap N_2)$. It follows from (vii) and Corollary 1 that it suffices to prove that N_1 is linearly disjoint from N_2. Let f be any $N_1 \cap N_2$-linear mapping of N_1 into K. By (ix) f can be represented in the form $\sum_{i=1}^{n} (a_r^i \phi_i) \mid N_1$, where $a^i \in K$ and $\phi_i \in G(K/N_1 \cap N_2)$,

[15] Cf. Theorem 3, p. 66 in [5].
[16] See [11] or [5].

for $i=1, 2, \cdots, n$. It follows from our assumption that for every ϕ_i, $i=1, 2,$ $\cdots, n$, there exists an automorphism $\psi_i \in G(K/N_2)$ such that $\phi_i | N_1 = \psi_i | N_1$. Therefore $f = \sum_{i=1}^{n} (a_r^i \psi_i) | N_1$. Hence f can be extended to a N_2-linear mapping $\sum_{i=1}^{n} a_r^i \psi_i$. Thus we have shown that every $(N_1 \cap N_2)$-linear mapping of N_1 into K can be extended to an N_2-linear mapping of K into K. Clearly, this implies that N_1 is linearly disjoint from N_2.

LEMMA 7. *Let K be a finite and normal extension of F and let N_1, N_2 be two division rings between F and K. If N_1 is linearly disjoint from N_2 and $Z(K, N_1 \cap N_2) = Z(K, N_2)$ then $G(N_1, K/N_1 \cap N_2) = G(K/N_2) | N_1$.*

Proof. Let $\phi \in G(N_1, K/N_1 \cap N_2)$. If N_1 is linearly disjoint from N_2 then ϕ can be extended to an N_2-linear mapping f of K into K. It follows from (viii) that f can be represented in the form $\sum_{i=1}^{n} a_r^i \phi_i$, where $\phi_i \in G(K/N_2)$ and $a^i \in K$, for $i = 1, \cdots, n$. Hence $\phi = \sum_{i=1}^{n} a_r^i (\phi_i | N_1)$. It follows from (x) that there exist an integer j, $1 \leq j \leq n$, and an element $a \in Z(K, N_1 \cap N_2)$ such that $\phi = I_a \cdot (\phi_j | N_1) = (I_a \phi_j) | N_1$. If $Z(K, N_1 \cap N_2) = Z(K, N_2)$, we have $I_a \in G(K/N_2)$, and hence $I_a \phi_j \in G(K/N_2)$. Thus $\phi \in G(K/N_2) | N_1$ and the lemma is proved.

THEOREM 3. *Let N_1, N_2 be two finite extensions of F, and let K be an extension of N_1, N_2, normal and finite over F, and suppose that $Z(K)$ is infinite. Every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(N_i, K/F)$, for $i = 1, 2$, has an extension $\phi \in G(K/F)$ if and only if N_1, N_2 are linearly disjoint and either $Z(K, N_1 \cap N_2) = Z(K, N_1)$ or $Z(K, N_1 \cap N_2) = Z(K, N_2)$.*

Proof. If N_1, N_2 are linearly disjoint and (e.g.) $Z(K, N_1 \cap N_2) = Z(K, N_2)$ then it follows from Lemma 7 that $G(N_1, K/N_1 \cap N_2) = G(K/N_2) | N_1$. Therefore, by Lemma 1, every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(N_i, K/F)$, $i = 1, 2$, has an extension $\phi \in G(K/F)$.

Conversely, let us suppose that every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(N_i, K/F)$, for $i = 1, 2$, has an extension $\phi \in G(K/F)$. Then it follows from Lemmas 1 and 6 that N_1, N_2 are linearly disjoint, and from Theorem 1 and (vii) that either $Z(K, N_1 \cap N_2) = Z(K, N_1)$ or $Z(K, N_1 \cap N_2) = Z(K, N_2)$. This completes the proof of the theorem.

Let N and M be two division subrings of K. Then we may consider K as an $(N; M)$-module. This module will be denoted by $_N K_M$.

COROLLARY 4. *Let K, M, N be finite and normal extensions of F such that $K = (M, N)$. Let $L = M \cap N$ and suppose that $Z(K)$ is infinite. If every compatible pair (ϕ_1, ϕ_2), where $\phi_1 \in G(M, K/F)$, $\phi_2 \in G(N, K/F)$, has an extension $\phi \in G(K/F)$ then the map $f: {}_M M_L \otimes_L {}_L N_N$, where $f(\sum_{i=1}^{r} x_i \otimes y_i) = \sum_{i=1}^{r} x_i y_i$, for every $x_i \in M$, $y_i \in N$, is an isomorphism of ${}_M M_L \otimes_L {}_L N_N$ onto ${}_M K_N$.*

Proof. Clearly, f is an $(M; N)$-homomorphism of ${}_M M_L \otimes_L {}_L N_N$ into ${}_M K_N$. Let $b_1, \cdots, b_n$ be a left L-basis of N. Then it follows from Theorem 3 that,

under the assumptions of our corollary, M and N are linearly disjoint. Hence $b_1, \cdots, b_n$ are left M-linearly independent. It follows that f is a monomorphism and that the left dimension of $f({}_M M_L \otimes_L {}_L N_N)$ over M is equal to $n = [N:L]$. Since M and N are normal over L, Corollary 3 and our assumption imply that $[K:M] = [N:L]$. Hence f is an epimorphism, and therefore an isomorphism of ${}_M M_L \otimes_L {}_L N_N$ onto ${}_M K_N$.

4. Letters A, B, B_1, B_2, C will, as before, denote simple rings with minimum condition. Let C, B be subrings of A and let B be between C and A. Then $D(B, A/C)$ denotes the set of all derivations of B into A mapping C into (0). Instead of $D(A, A/C)$ we shall write $D(A/C)$. If $a \in A$ then the map d_a defined by $d_a(x) = ax - xa$, for all $x \in A$, is a derivation. d_a is an element of $D(A/C)$ if and only if $a \in Z(A, C)$.

In the sequel we shall use the following theorem:

(xi)[17] Let A be a Galois extension of C and B be between C and A. If $d \in D(B, A/C)$ then there exists $a \in Z(A, C)$ such that $d_a | B = d$. In particular every derivation $d \in D(A/C)$ is inner.

Let C, B_1, B_2 be subrings of A and let B_1, B_2 be between C and A. If $d_i \in D(B_i, A/C)$, for $i = 1, 2$, then an element $d \in D(A/C)$ is called an extension of the pair (d_1, d_2) if $d | B_i = d_i$, for $i = 1, 2$. The pair (d_1, d_2) is called compatible if $d_1 | B_1 \cap B_2 = d_2 | B_1 \cap B_2$.

LEMMA 8. *Let A be a Galois extension of C and let B_1, B_2 be between C and A. Then the following three conditions are equivalent:*

(a) *every compatible pair (d_1, d_2), where $d_i \in D(B_i, A/C)$, for $i = 1, 2$ has an extension $d \in D(A/C)$.*

(b) $D(A/B_1 \cap B_2) = D(A/B_1) + D(A/B_2)$.

(c) $Z(A, B_1 \cap B_2) = Z(A, B_1) + Z(A, B_2)$.

Proof. (a)$\Rightarrow$(b). Let $d \in D(A/B_1 \cap B_2)$. It follows from (a) that there exists a derivation $d_1 \in D(A/C)$ such that $d_1 | B_2 = d | B_2$ and $d_1 | B_1$ is the zero derivation of B_1. Now $d = d_1 + (d - d_1)$, $d - d_1 \in D(A/B_2)$ and $d_1 \in D(A/B_1)$. Thus $d \in D(A/B_1) + D(A/B_2)$.

(b)$\Rightarrow$(c). Let $c \in Z(A, B_1 \cap B_2)$. Then $d_c \in D(A/B_1 \cap B_2)$. Hence d_c can be represented in the form $d' + d''$ where $d' \in D(A/B_1)$ and $d'' \in D(A/B_2)$. It follows from (xi) that d' and d'' are inner. Hence there exist elements a and b such that $d_c = d_a + d_b$, $d_a = d' \in D(A/B_1)$ and $d_b = d'' \in D(A/B_2)$. Therefore $a \in Z(A, B_1)$, $b \in Z(A, B_2)$ and $c = a + b + z$ where $z \in Z(A)$. Thus $c \in Z(A, B_1) + Z(A, B_2)$.

(c)$\Rightarrow$(a). Let us take (d_1, d_2) as in (a). It follows from (xi) that there exists $a \in Z(A, C)$ and $a_1, a_2 \in Z(A, B_1 \cap B_2)$ such that $d | B_1 \cap B_2 = d_a | B_1 \cap B_2$ and $d_{a_i} | B_i = d_i - d_a$, for $i = 1, 2$. a_1 and a_2 can be represented in the form $a_1 = a_1' + a_1''$, $a_2 = a_2' + a_2''$, where a_1', $a_2' \in Z(A, B_1)$ and a_1'', $a_2'' \in Z(A, B_2)$. Let $b = a_1'' + a_2'$. Then

---

[17] (xi) is a particular case of Theorem 1, p. 151 in [12].

$$d_b \mid B_1 = d_{a''_1} \mid B_1 = d_{a_1} \mid B_1 = d_1 - (d_a \mid B_1),$$

$$d_b \mid B_2 = d_{a'_2} \mid B_2 = d_{a_2} \mid B_2 = d_2 - (d_a \mid B_2).$$

Therefore $d_b + d_a$ is an extension of (d_1, d_2) to a derivation of A.

LEMMA 9. *Let R be an arbitrary ring with 1 and let B_1, B_2, C be simple subrings of R satisfying the minimum condition and containing 1. If $B_1 \cap B_2 \subset C$, $[R:C] < \infty$ and $R = B_1 + B_2$ then either $R = B_1$ or $R = B_2$.*

Proof. There exists a division ring L such that $[C:L] < \infty$, and we may suppose that $[B_1:L] \geqq [B_2:L]$. Then we have $[R:L] \leqq [B_1:L] + [B_2:L] - 1 < 2[B_1:L]$, since $R = B_1 + B_2$. On the other hand, $[R:L] = [R:B_1][B_1:L]$. Therefore $[R:B_1] < 2$. Hence $[R:B_1] = 1$ and so $R = B_1$.

THEOREM 4. *Let A be a Galois extension of C and let B_1, B_2 be two regular subrings of A containing C. Then the following three conditions are equivalent:*

(a) *every compatible pair (d_1, d_2), where $d_i \in D(B_i, A/C)$, for $i = 1, 2$, has an extension $d \in D(A/C)$.*

(b) $D(B_1, A/B_1 \cap B_2) = 0$ *or* $D(B_2, A/B_1 \cap B_2) = 0$.

(c) $Z(A, B_1 \cap B_2) = Z(A, B_1)$ *or* $Z(A, B_1 \cap B_2) = Z(A, B_2)$.

Proof. It is easy to see that (b)$\Rightarrow$(c). By (xi), (c)$\Rightarrow$(b). Hence it suffices to prove that (a)$\Rightarrow$(c) and (b)$\Rightarrow$(a).

(a)$\Rightarrow$(c). If every compatible pair (d_1, d_2), where $d_i \in D(B_i, A/C)$, for $i = 1, 2$, has an extension $d \in D(A/C)$ then it follows from Lemma 8 that $Z(A, B_1) + Z(A, B_2) = Z(A, B_1 \cap B_2)$. Next, $Z(A, B_1)$ and $Z(A, B_2)$ are simple rings with minimum condition, $Z(A, B_1) \cap Z(A, B_2) \subset Z(A)$ and

$$[Z(A, B_1 \cap B_2) : Z(A)] \leqq [Z(A, C) : Z(A)] < \infty.$$

Therefore, it follows from Lemma 9 that either $Z(A, B_1 \cap B_2) = Z(A, B_1)$ or $Z(A, B_1 \cap B_2) = Z(A, B_2)$.

(b)$\Rightarrow$(a). Let us suppose that $D(B_1, A/B_1 \cap B_2) = 0$ and let (d_1, d_2) be a pair as in (a). It follows from (xi) that there exists a derivation $d \in D(A/C)$ such that $d \mid B_2 = d_2$. Then $(d \mid B_1) - d_1 \in D(B_1, A/B_1 \cap B_2)$. Hence $(d \mid B_1) - d_1 = 0$, and d is an extension of the pair (d_1, d_2).

COROLLARY 5. *Let A, B_1, B_2, C be as in Theorem 4 and let $Z(A)$ be infinite. If every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for $i = 1, 2$, has an extension $\phi \in G(A/C)$ then every compatible pair (d_1, d_2), where $d_i \in D(B_i, A/C)$, for $i = 1, 2$, has an extension $d \in D(A/C)$.*

The foregoing corollary is an immediate consequence of Theorem 1 and Theorem 4.

COROLLARY 6. *Let A, B_1, B_2, C be as in Corollary 5 and let B_1, B_2 be normal extensions of $B_1 \cap B_2$. Every compatible pair (ϕ_1, ϕ_2), where $\phi_i \in G(B_i, A/C)$, for*

$i = 1, 2$, *has an extension* $\phi \in G(A/C)$ *if and only if every compatible pair* (d_1, d_2), *where* $d_i \in D(B_i, A/C)$, *for* $i = 1, 2$, *has an extension* $d \in D(A/C)$.

The above corollary is a consequence of Corollary 5, Theorem 4, and Theorem 2.

5. In this part we shall prove the following two theorems, where A, B, C are simple rings with minimum condition.

THEOREM 5. *Let* C *be a regular subring of* A, *let* B *be between* C *and* A *and suppose that* $Z(A)$ *is infinite. If* $\phi(B) = B$ *for every* $\phi \in G(A/C)^0$ *then either* $B \subset A^{G(A/C)^0}$ *or* $Z(A, C) \subset B$.

THEOREM 6. *Let* A *be a Galois extension of* C, *let* B *be a subring between* C *and* A, *and suppose that* $Z(A)$ *is infinite. Then* B *is an* A-*normal extension of* C *if and only if* B *is a normal extension of* C *and either* $B \subset A^{G(A/C)^0}$ *or* $Z(A, C) \subset B$.

As before, A, B, C will stand for simple rings with minimum condition.

LEMMA 10. *Let* C *be a subring of* A, *and let* B *be between* C *and* A. *Then* $[Z(A, C):Z(B)] < \infty$. *Moreover, if* $Z(A)$ *is infinite then* $Z(B)$ *is also infinite.*

Proof. It follows from (iii) that $[Z(A, C):Z(A)] < \infty$ and $[Z(A, B):Z(B)] \leq [A:B] \leq [A:C] < \infty$. On the other hand, $Z(A, B) \supset Z(A)$. Hence $[Z(A, C):Z(B)] < \infty$. Thus the first part of the lemma is proved. Now if $Z(B)$ is finite then $Z(A, C)$ is finite and so $Z(A)$ is finite. This completes the proof of the lemma.

Let $C \subset B \subset A$ be successive extensions of C. Then $H(A/C, B)$ denotes the subgroup of $G(A/C)$ composed of all elements I_a, where $a \in Z(A, B)^* \cdot Z(B, C)^*$. Let $G(A/C, B)$ denote the subgroup of $G(A/C)$ consisting of the elements of $G(A/C)$ that map B onto itself. Clearly, $H(A/C, B)$ is a normal subgroup of $G(A/C, B)$.

LEMMA 11. *Let* A *be a finite extension of* C *and let* B *be between* C *and* A. *Then*

$$[G(A/C, B):H(A/C, B)] = [G(A/B):G(A/B)^0] \cdot [G(A/C, B) \mid B:G(B/C)^0].$$

Proof. Let $\{\psi_1, \cdots, \psi_m\}$ be a set of representatives of the cosets of $G(A/B)^0$ in $G(A/B)$ and let $\{\phi_1, \cdots, \phi_n\}$ be a subset of $G(A/C)$ such that $\{\phi_1 \mid B, \cdots, \phi_n \mid B\}$ is a set of representatives of the cosets of $G(B/C)^0$ in $G(A/C, B) \mid B$. (It follows from (iii) that the sets are finite.) Let $\phi \in G(A/C, B)$. Then there exists $a \in Z(B, C)^*$ and an integer i, $1 \leq i \leq n$, such that $\phi \mid B = (\phi_i I_a) \mid B$. Thus $\phi(\phi_i I_a)^{-1} \in G(A/B)$ and hence there exist $b \in Z(A, B)^*$ and an integer j, $1 \leq j \leq m$, such that $\phi(\phi_i I_a)^{-1} = \psi_j I_b$. Therefore $\phi = \psi_j I_b \phi_i I_a = \psi_j \phi_i I_{\phi_i^{-1}(b)} I_a$. But $\phi_i^{-1}(B) = B$ and so $\phi_i^{-1}(Z(A, B)^*) = Z(A, B)^*$. Hence we have proved that every element $\phi \in G(A/C, B)$ can be represented in the

form $\psi_j\phi_i I_c$, where $1 \leq j \leq m$, $1 \leq i \leq n$ and $c \in Z(A, B)^* \cdot Z(B, C)^*$. Thus $G(A/C, B) = \bigcup_{i,j} \psi_j\phi_i H(A/C, B)$. But it is easy to see that $\psi_{j_1}\phi_{i_1}$ and $\psi_{j_2}\phi_{i_2}$ belong to the same coset of $H(A/C, B)$ in $G(A/C, B)$ if and only if $j_1 = j_2$ and $i_1 = i_2$. Hence

$$[G(A/C, B):H(A/C, B)] = m \cdot n = [G(A/B):G(A/B)^0][G(A/C, B)B:G(B/C)^0].$$

LEMMA 12. *Let R be a ring with the identity* 1, *let F be an infinite subfield of R containing* 1 *and suppose that* $[R: F] < \infty$. *Let P be a subring between F and R. If $[R^*: P^*] < \infty$ then $R = P$.*

Proof. We shall consider R and P as left F-vector spaces. Let us suppose that $[R^*: P^*] < \infty$. Then there exists a finite subset $\{a_i\}_{i=1,\dots,n}$ of R^* such that $R^* = \bigcup_{i=1}^{n} P^* a_i$. Therefore $(R^*)^- = \bigcup_{i=1}^{n} (P^*)^- a_i$. But it follows from Lemma 2 that $(R^*)^- = R$ and $(P^*)^- = P$. Hence $R = \bigcup_{i=1}^{n} P a_i$ and so $R = P a_j$ for some j, $1 \leq j \leq n$. Therefore $P = R a_j^{-1} = R$ and the proof of the lemma is finished.

REMARKS. The following generalization of the lemma is still true:

Let R be a ring with the identity 1, let F be an infinite subfield of R containing 1 and suppose that $[R: F] < \infty$. Let P be a subring of R. If $[R^*: P^*] < \infty$ then $R = P$.

On the other hand the lemma does not remain true if we omit the assumption $[R: F] < \infty$, even in the case where R is a commutative ring.

One can also prove the following theorem:

Let R be an infinite simple ring with minimum condition and let P be a subring of R. If $[R^*: P^*] < \infty$ then $R = P$.

Proof of Theorem 5. Let us suppose that B is carried into itself by every inner automorphism belonging to $G(A/C)$. Then $Z(A, B)$ and $Z(B, C)$ are carried into themselves by every inner automorphism of $Z(A, C)$. Moreover, $G(A/C)^0 \subset G(A/C, B)$ and hence it follows from Lemma 12 that $H(A/C, B)$ is of finite index in $G(A/C)^0$. Therefore $[Z(A, C)^*: Z(A, B)^* \cdot Z(B, C)^*] < \infty$. Furthermore $Z(A, B) \supset Z(B)$ and $Z(B, C) \supset Z(B)$ and it follows from Lemma 11 that $[Z(A, C): Z(B)] < \infty$ and that $Z(B)$ is infinite. Now, $Z(A, B)$ and $Z(B, C)$ are semisimple rings with minimum condition. Indeed, $[Z(A, B): Z(B)] < \infty$ and $[Z(B, C): Z(B)] < \infty$ and hence $Z(A, B)$, $Z(B, C)$ satisfy the minimum condition. Moreover, if R is the radical of $Z(A, B)$ then $aRa^{-1} \subset R$ for every $a \in Z(A, C)^*$ (since $aZ(A, B)a^{-1} \subset Z(A, B)$ for every $a \in Z(A, C)^*$). Hence $Z(A, C)R \subset RZ(A, C)$ because every element from $Z(A, C)$ can be represented as a sum of units. Therefore $Z(A, C)RZ(A, C)$ is nilpotent and hence 0. Thus $R = 0$. Similarly, the radical of $Z(B, C)$ is trivial. Now, if $a \in Z(A, B)$, $b \in Z(B, C)$ then $ab = ba$ and it follows from Lemma 12 that $(Z(A, B), Z(B, C)) = Z(A, C)$. Therefore $Z(B) \subset Z(Z(A, C))$, $Z(Z(A, B)) \subset Z(Z(A, C))$ and $Z(Z(B, C)) \subset Z(Z(A, C))$. But $Z(Z(A, C))$ is a field. Hence $Z(A, B)$ and $Z(B, C)$ are simple rings with minimum condition. Therefore it follows from Lemma 4 that either $Z(A, C) = Z(A, B)$ are $Z(A, C) = Z(B, C)$. If $Z(A, C)$

$=Z(A, B)$ then $B \subset A^{G(A/C)^0}$. If $Z(A, C) = Z(B, C)$ then $Z(A, C) \subset B$. Therefore the theorem is proved([18]).

COROLLARY 7. *Let C be a regular subring of A, let B be between C and A and suppose that $Z(A)$ is infinite. If B is carried into itself by every inner automorphism belonging to $G(A/C)$ then B is a regular subring of A.*

Proof. It follows from Theorem 5 that if B is carried into itself by every inner automorphism belonging to $G(A/C)$ then either $B \subset A^{G(A/C)^0}$ or $Z(A, C) \subset B$. Suppose that $B \subset A^{G(A/C)^0}$. Then $Z(A, C) = Z(A, B)$. Therefore $Z(A, B)$ is a simple ring. Moreover $[A:B] \leq [A:C] < \infty$. Hence B is a regular subring of A. Now, let us suppose that $Z(A, C) \subset B$. Then $Z(A, B) = Z(B)$. Therefore $Z(A, B)$ is a field. But, as before, $[A:B] \leq [A:C] < \infty$. Hence B is a regular subring of A. This completes the proof of the corollary.

Proof of Theorem 6. If B is a A-normal extension of C then B is a normal extension of C and, by Theorem 5, either $B \subset A^{G(A/C)^0}$ or $Z(A, C) \subset B$.

Let B be a normal extension of C and $B \subset A^{G(A/C)^0}$. Then B is a regular subring of A, since $Z(A, B) = Z(A, C)$. Hence, it follows from Lemma 5, that B is an A-normal extension of C.

Now, let $Z(A, C) \subset B$. Then $H(A/C, B) = G(A/C)^0$ and, by Lemma 11, $[G(A/C, B) : G(A/C)^0] = [G(A/B) : G(A/B)^0][G(A/C, B) | B : G(B/C)^0]$.

On the other hand B is a Galois extension of C because $Z(A, C) = Z(B, C)$, $[G(B/C) : G(B/C)^0] \leq [B:C] < \infty$ and B is a normal extension of C. Next B is a regular subring of A since $Z(A, B) = Z(B)$. Hence $G(A/C, B) | B = G(B, C)$ and

$$[G(A/C):G(A/C)^0] = \frac{[A:C]}{[Z(A,C):Z(A)]} = \frac{[A:B][B:C]}{[Z(A,C):Z(A)]}$$

$$= \frac{[G(A/B):G(A/B)^0][Z(A,B):Z(A)][G(B/C):G(B/C)^0][Z(B,C):Z(B)]}{[Z(A,C):Z(A)]}$$

$$= \frac{[Z(B):Z(A)][Z(A,C):Z(B)]}{[Z(A,C):Z(A)]}[G(A/B):G(A/B)^0][G(B/C):G(B/C)^0]$$

$$= [G(A/B):G(A/B)^0][G(B/C):G(B/C)^0].$$

Therefore $G(A/C) = G(A/C, B)$. Hence B is an A-normal extension of C. The proof is complete.

COROLLARY 8. *Let A be a Galois extension of C, let $G(A/C) = G(A/C)^0$ and suppose that $Z(A)$ is infinite. If B is an A-normal extension of C then either $B = A$ or $B = C$.*

The above corollary is an immediate consequence of Theorem 6.

([18]) One can get a somewhat shorter proof of the theorem applying Theorem 1, p. 121 in [6] (Cf. Theorem 3, p. 863 in [2]) or Satz 3, p. 186 in [13] (Cf. also Theorem 3, p. 191 in [10]).

REFERENCES

1. S. A. Amitsur, *Invariant submodules of simple rings*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 987–989.

2. W. E. Baxter, *Lie simplicity of a special class of associative rings*, Proc. Amer. Math. Soc. vol. 7 (1957) pp. 855–863.

3. N. Bourbaki, *Algèbre*, Livre II, Chapitre 8, Paris, Hermann, 1958.

4. R. Brauer, *On a theorem of H. Cartan*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 619–620.

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

6. A. Hattori, *On invariant subrings*, Jap. J. Math. vol. 21 (1951) pp. 121–130.

7. G. P. Hochschild, *Double vector spaces over division rings*, Amer. J. Math. vol. 71 (1949) pp. 443–460.

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

9. L. K. Hua, *Some properties of sfield*, Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1949) pp. 533–537.

10. ———, *A note on the total matrix ring over a non-commutative field*, Ann. Soc. Polon. Math. vol. 25 (1952) pp. 188–198.

11. N. Jacobson, *A note on division rings*, Amer. J. Math. vol. 69 (1947) pp. 27–36.

12. ———, *Structure of rings*, Amer. Math. Soc. Colloquium Publications, vol. 37, Providence, 1956.

13. F. Kasch, *Invariante Untermoduln des Endomorphismenrings eines Vektorraums*, Arch. Math. vol. 4 (1953) pp. 182–190.

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

15. A. Rosenberg, *The Cartan-Brauer-Hua theorem for matrix and local matrix rings*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 891–898.

UNIVERSITY OF CALIFORNIA,
    BERKELEY, CALIFORNIA
POLISH ACADEMY OF SCIENCES,
    WARSAW, POLAND