GALOIS THEORY AND THE EXISTENCE OF MAXIMAL UNRAMIFIED SUBALGEBRAS

H. F. KREIMER

ABSTRACT. Let $B$ be a commutative ring with 1, let $G$ be a finite group of automorphisms of $B$, and let $A$ be the subring of $G$-invariant elements of $B$. There exists a $G$-stable, unramified $A$-subalgebra of $B$ which contains every unramified $A$-subalgebra of $B$.

Throughout this paper $B$ will denote a given commutative ring with 1. $G$ will denote a given finite group of automorphisms of $B$, and $A$ will denote the subring of $G$-invariant elements of $B$. Following the terminology of [1], an $A$-subalgebra $A'$ of $B$ will be called unramified if $A_p'/pA_p'$ is a separable algebra over $A_p'/pA_p$ for every prime ideal $p$ in $A$, where $A_p$ (resp. $A_p'$) is the ring of fractions of $A$ (resp. $A'$) with respect to the complement of $p$ in $A$.

Lemma. Let $m$ be a maximal ideal of $A$, and suppose $A'$ is an $A$-subalgebra of $B$ such that $A'/A'm$ is a separable $A/m$-algebra.

(i) The homomorphism of $A'/A'm$ into $B/Bm$ induced by the inclusion map of $A'$ into $B$ is an injection, by which $A'/A'm$ may be identified with a subalgebra of $B/Bm$.

(ii) The dimension of the algebra $A'/A'm$ over the field $A/m$ does not exceed the order of $G$.

(iii) $A'/A'm$ and the subring of $G$-invariant elements of $B/Bm$ are linearly disjoint subalgebras of the $A/m$-algebra $B/Bm$.

Proof. Note that $A'/A'm$ is a finite-dimensional algebra over the field $A/m$. More generally, a separable algebra over a commutative ring which is a projective module over that ring is finitely generated as a module by [6, Proposition 1.1]. Therefore $A'/A'm$ is a semisimple algebra by [4, Chapter
IX, Proposition 7.7 and Theorem 7.10], and $A' \mathfrak{m}$ must equal the intersection of the maximal ideals of $A'$ which contain it. Since $B$ is integral over $A$ [3, Chapter V, §1, Proposition 22], $B$ is integral over $A'$. Since every prime ideal of $A'$ is the contraction of a prime ideal of $B$ [3, Chapter V, §2, Theorem 1], it follows that $A' \mathfrak{m}$ is the contraction of some ideal $\mathfrak{m}'$ of $B$, $Bm \subseteq \mathfrak{m}'$, and $A' \cap Bm \subseteq A' \cap \mathfrak{m}' = A' \mathfrak{m}$. But obviously $A' \mathfrak{m} \subseteq A' \cap Bm$ and, therefore, $A' \mathfrak{m} = A' \cap Bm$ and the homomorphism of $A'/A' \mathfrak{m}$ into $B/Bm$ induced by the inclusion map of $A'$ into $B$ is injective.

Let $B' = \prod_{\sigma \in G} \sigma(A')$, and let $H$ be the group of automorphisms of $B'$ which are restrictions of elements of $G$. Since each element $\sigma$ of $G$ induces an $A/m$-algebra isomorphism of $A'/A' \mathfrak{m}$ onto $\sigma(A')/\sigma(A') \mathfrak{m}$, $\sigma(A')/\sigma(A') \mathfrak{m}$ is again a separable $A/m$-algebra, and $B'/B' \mathfrak{m}$, which is a homomorphic image of the tensor product of the $A/m$-algebras $\sigma(A')/\sigma(A') \mathfrak{m}$, $\sigma \in G$, is a separable algebra over $A/m$ by [2, Propositions 1.4 and 1.5]. Consequently, $B' \mathfrak{m}$ must equal the intersection of the maximal ideals of $B'$ which contain it. Because $\mathfrak{m}$ is a maximal ideal of $A$, the set of maximal ideals of $B'$ which contain $B' \mathfrak{m}$ coincides with the set of maximal ideals of $B'$ which lie over $\mathfrak{m}$. Choose a maximal ideal $\mathfrak{m}'$ of $B'$ which lies over $\mathfrak{m}$, let $H^Z(\mathfrak{m}')$ be the subgroup of $\sigma \in H$ such that $\sigma(\mathfrak{m}') \subseteq \mathfrak{m}'$, and let $H^T(\mathfrak{m}')$ be the subgroup of $\sigma \in H^Z(\mathfrak{m}')$ which induces the identity automorphism on $B'/\mathfrak{m}'$. By [3, Chapter V, §2, Theorem 2], $H$ acts transitively on the set of all prime ideals of $B'$ which lie over $\mathfrak{m}$, and $B'/\mathfrak{m}'$ is a normal field extension of $A/m$ with Galois group isomorphic to the quotient group $H^Z(\mathfrak{m}')/H^T(\mathfrak{m}')$. Therefore the prime ideals of $B'$ which lie over $\mathfrak{m}$ are maximal, their number is finite and equal to $(H : H^Z(\mathfrak{m}'))$, and $B'/\mathfrak{m}'$ is isomorphic to $B'/\mathfrak{m}'$ for every maximal ideal $\mathfrak{m}$ of $B'$ which lies over $\mathfrak{m}$. $B'/\mathfrak{m}'$ is a separable field extension of $A/m$ by [2, Proposition 1.4], and so the dimension of $B'/\mathfrak{m}'$ over $A/m$ is equal to the order of the Galois group of $B'/\mathfrak{m}'$ over $A/m$. Letting $\mathfrak{m}$ range over the set of maximal ideals of $B'$ which contract to $\mathfrak{m}$, $B'/B' \mathfrak{m}$ is isomorphic to the direct product of the fields $B'/\mathfrak{m}$ [3, Chapter II, §1, Proposition 5], and the dimension of $B'/B' \mathfrak{m}$ over $A/m$ must equal

$$[H : H^Z(\mathfrak{m}')] \cdot [H^Z(\mathfrak{m}'): H^T(\mathfrak{m}')] = [H : H^T(\mathfrak{m}')]$$

Use the homomorphisms induced by the inclusion maps of $A'$ into $B'$ and $B'$ into $B$ to identify $B'/B' \mathfrak{m}$ with a subalgebra of $B/Bm$ and $A'/A' \mathfrak{m}$ with a subalgebra of $B'/B' \mathfrak{m}$. Then neither the dimension of the $A/m$-algebra $B'/B' \mathfrak{m}$ nor the dimension of its subalgebra $A'/A' \mathfrak{m}$ can exceed the order of $G$. License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Finally, letting $\overline{A}$ be the subring of $G$-invariant elements of $B/Bm$, it is evident that $\overline{A}$ is an $A/m$-algebra. If the canonical homomorphism of $(B'/B'm) \otimes_{A/m} \overline{A}$ into $B/Bm$, which maps $b \otimes a$ onto $ba$ for $b \in B'/B'm$ and $a \in \overline{A}$, is injective, then $B'/B'm$ and $\overline{A}$ are linearly disjoint subalgebras of the $A/m$-algebra $B/Bm$, and, consequently, so are $A'/A'm$ and $A$. But $B/Bm \cong (B'/B'm) \otimes_{B'} B$, and it has been noted already that $B'/B'm$ is a direct product of the fields $B'/\mathfrak{m}$ ranging over the set of maximal ideals of $B'$ which contract to $m$. Therefore, letting $\mathfrak{m}_0$ be any given maximal ideal of $B'$ which lies over $m$, it is sufficient to prove that the canonical homomorphism $\pi$ of $(B'/\mathfrak{m}_0) \otimes_{A/m} \overline{A}$ into $B/B\mathfrak{m}_0 \cong (B'/\mathfrak{m}_0) \otimes_{B'} B$, which maps $b \otimes a$ onto $ba$ for $b \in B'/\mathfrak{m}_0$ and $a \in \overline{A}$, is injective. Since $B'/\mathfrak{m}_0$ is a normal, separable field extension of $A/m$ with Galois group $H^2(\mathfrak{m}_0)/H^1(\mathfrak{m}_0)$, there exist a positive integer $n$ and elements $x_i, y_i$ of $B'/\mathfrak{m}_0, 1 \leq i \leq n$, such that $\sum_{i=1}^n x_i \cdot \rho(y_i) = \delta_{i, \rho}$ for all $\rho \in H^2(\mathfrak{m}_0)/H^1(\mathfrak{m}_0)$ by [5, Theorem 1.3]. Letting $\tau \in H^1(\mathfrak{m}_0)$ and letting $\sigma$ be an element of $G$ which extends $\tau$, $\sigma$ induces an $A$-algebra automorphism on the image of $\pi$, and in this way $H^2(\mathfrak{m}_0)$ is represented as a group of automorphisms of the image of $\pi$. Moreover, $H^1(\mathfrak{m}_0)$ is the kernel of this representation, and thus $H^2(\mathfrak{m}_0)/H^1(\mathfrak{m}_0)$ is represented as a group of $A$-algebra automorphisms of the image of $\pi$. For any element $c$ of the image of $\pi$, let $\text{tr}(c)$ be the sum of the elements $\rho(c), \rho \in H^2(\mathfrak{m}_0)/H^1(\mathfrak{m}_0)$, and notice that, if $c \in B'/\mathfrak{m}_0$, then $\text{tr}(c) \in A/m$. If $b \in B'/\mathfrak{m}_0$ and $a \in \overline{A}$, then

$$b \otimes a = \sum_{i=1}^n x_i \cdot \text{tr}(y_i b) \otimes a = \sum_{i=1}^n x_i \otimes \text{tr}(y_i ba) \quad \text{in} \quad (B'/\mathfrak{m}_0) \otimes_{A/m} \overline{A};$$

and from this formula it follows easily that $\pi$ is injective.

**Theorem.** There exists an unramified $A$-subalgebra of $B$ which is stable under $G$ and contains every unramified $A$-subalgebra of $B$.

**Proof.** Let $\mathfrak{p}$ be any prime ideal of $A$, and let $A'$ be an unramified $A$-subalgebra of $B$. Then $A_{\mathfrak{p}}'$ is the subring of $G$-invariant elements of $B_{\mathfrak{p}}$ by [3, Chapter V, §1, Proposition 23], $\mathfrak{p}A_{\mathfrak{p}}'$ is a maximal ideal of $A_{\mathfrak{p}}'$, and $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$ is a separable $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$-algebra. Therefore, the inclusion map of $A_{\mathfrak{p}}'$ into $B_{\mathfrak{p}}$ induces a monomorphism by which $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$ may be identified with a subalgebra of $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ and the dimension of $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$ over $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$ does not exceed the order of $G$ by the preceding lemma. Partially order the unramified $A$-subalgebras of $B$ by inclusion, let $\mathcal{F}$ be a chain of unramified $A$-subalgebras of $B$, and let $\overline{A} = \bigcup_{A' \in \mathcal{F}} A'$. Choose an element $A'$ of $\mathcal{F}$ for which the dimension of $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$ over $A_{\mathfrak{p}}'/\mathfrak{p}A_{\mathfrak{p}}'$
is greatest. If \( B' \) is an element of \( \mathcal{F} \) such that \( A' \subseteq B' \), then the dimensions of the \( A_p / \mathfrak{p} A_p \)-algebras \( A'_p / \mathfrak{p} A'_p \) and \( B'_p / \mathfrak{p} B'_p \) must be equal, and therefore \( A'_p / \mathfrak{p} A'_p = B'_p / \mathfrak{p} B'_p \). Consequently, \( A_p / \mathfrak{p} A_p = A'_p / \mathfrak{p} A'_p \), and so \( A_p / \mathfrak{p} A_p \) is a separable \( A_p / \mathfrak{p} A_p \)-algebra. Thus \( A \) is an unramified \( A \)-subalgebra of \( B \), and certainly it is an upper bound for \( \mathcal{F} \). By Zorn's lemma, there exists a maximal unramified \( A \)-subalgebra \( C \) of \( B \). If \( A' \) is any unramified \( A \)-subalgebra of \( B \), then \( (A' C)_p / \mathfrak{p} (A' C)_p \), which is a homomorphic image of the tensor product of the \( A_p / \mathfrak{p} A_p \)-algebras \( A'_p / \mathfrak{p} A'_p \) and \( C_p / \mathfrak{p} C_p \), is a separable algebra over \( A_p / \mathfrak{p} A_p \) for any prime ideal \( \mathfrak{p} \) of \( A \), and consequently \( A' C \) is an unramified \( A \)-subalgebra of \( B \) which contains \( C \). Therefore, \( A' C = C \) and \( A' \subseteq C \). If \( \sigma \in G \), then \( \sigma(C) \) is again an unramified \( A \)-algebra, and so \( \sigma(C) \subseteq C \). Therefore, \( C \) is stable under \( G \).

REFERENCES


DEPARTMENT OF MATHEMATICS, FLORIDA STATE UNIVERSITY, TALLAHASSEE, FLORIDA 32306