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 $A'_p/\mathfrak{p}A'_p$ is a separable algebra over $A_p/\mathfrak{p}A_p$ for every prime ideal $\mathfrak{p}$ in $A$, where $A_p$ (resp. $A'_p$) is the ring of fractions of $A$ (resp. $A'$) with respect to the complement of $\mathfrak{p}$ 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 3].
IX, Proposition 7.7 and Theorem 7.10], and $A^{'m}$ 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 $A^{'m}$ is the contraction of some ideal $\mathfrak{p}$ of $B$, $B^{'m} \subseteq \mathfrak{p}$, and $A' \cap B^{'m} \subseteq A' \cap \mathfrak{p} = A^{'m}$. But obviously $A^{'m} \subseteq A' \cap B^{'m}$ and, therefore, $A^{'m} = A' \cap B^{'m}$ and the homomorphism of $A'/A^{'m}$ into $B/B^{'m}$ induced by the inclusion map of $A'$ into $B$ is injective.

Let $B' = \Pi_{\sigma\in G} \sigma(A')$, 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 $A'/A^{'m}$ onto $\sigma(A')/\sigma(A^{'m})$, $\sigma(A')/\sigma(A^{'m})$ is a separable $A/m$-algebra, and $B'/B^{'m}$, which is a homomorphic image of the tensor product of the $A/m$-algebras $\sigma(A')/\sigma(A^{'m})$, $\sigma \in G$, is a separable algebra over $A/m$ by [2, Propositions 1.4 and 1.5]. Consequently, $B^{'m}$ must equal the intersection of the maximal ideals of $B'$ which contain it. Because $m$ is a maximal ideal of $A$, the set of maximal ideals of $B'$ which contain $B^{'m}$ coincides with the set of maximal ideals of $B'$ which lie over $m$. Choose a maximal ideal $\mathfrak{m}_0$ of $B'$ which lies over $m$, let $H^Z(\mathfrak{m}_0)$ be the subgroup of $\sigma \in H$ such that $\sigma(\mathfrak{m}_0) \subseteq \mathfrak{m}_0$, and let $H^T(\mathfrak{m}_0)$ be the subgroup of $\sigma \in H^Z(\mathfrak{m}_0)$ which induces the identity automorphism on $B'/\mathfrak{m}_0$. By [3, Chapter V, §2, Theorem 2], $H$ acts transitively on the set of all prime ideals of $B'$ which lie over $m$, and $B'/\mathfrak{m}_0$ is a normal field extension of $A/m$ with Galois group isomorphic to the quotient group $H^Z(\mathfrak{m}_0)/H^T(\mathfrak{m}_0)$. Therefore the prime ideals of $B'$ which lie over $m$ are maximal, their number is finite and equal to $(H: H^Z(\mathfrak{m}_0))$, and $B'/\mathfrak{m}$ is isomorphic to $B'/\mathfrak{m}_0$ for every maximal ideal $\mathfrak{m}$ of $B'$ which lies over $m$. $B'/\mathfrak{m}_0$ is a separable field extension of $A/m$ by [2, Proposition 1.4], and so the dimension of $B'/\mathfrak{m}_0$ over $A/m$ is equal to the order of the Galois group of $B'/\mathfrak{m}_0$ over $A/m$. Letting $\mathfrak{m}$ range over the set of maximal ideals of $B'$ which contract to $m$, $B'/B^{'m}$ is isomorphic to the direct product of the fields $B'/\mathfrak{m}$ [3, Chapter II, §1, Proposition 5], and the dimension of $B'/B^{'m}$ over $A/m$ must equal

$$[H:H^Z(\mathfrak{m}_0)] \cdot [H^Z(\mathfrak{m}_0):H^T(\mathfrak{m}_0)] = [H:H^T(\mathfrak{m}_0)].$$

Use the homomorphisms induced by the inclusion maps of $A'$ into $B'$ and $B'$ into $B$ to identify $B'/B^{'m}$ with a subalgebra of $B/B^{'m}$ and $A'/A^{'m}$ with a subalgebra of $B'/B^{'m}$. Then neither the dimension of the $A/m$-algebra $B'/B^{'m}$ nor the dimension of its subalgebra $A'/A^{'m}$ can exceed the order of $G$.
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 $B'/\mathfrak{m}'$, $\mathfrak{m}'$ 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 $H^Z(\mathfrak{m}_0)/HT(\mathfrak{m}_0)$, there exist a positive integer $n$ and elements $x_i, y_i$ of $B'/\mathfrak{m}_0$, $1 \leq i \leq n$, such that $\sum_{i=1}^n x_i \cdotp \rho(y_i) = \delta_{1,\rho}$ for all $\rho \in H^Z(\mathfrak{m}_0)/HT(\mathfrak{m}_0)$ by [5, Theorem 1.3]. Letting $\tau \in H^Z(\mathfrak{m}_0)$ 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 $H^Z(\mathfrak{m}_0)$ is represented as a group of automorphisms of the image of $\pi$. Moreover, $H^T(\mathfrak{m}_0)$ is the kernel of this representation, and thus $H^Z(\mathfrak{m}_0)/HT(\mathfrak{m}_0)$ is represented as a group of $\overline{A}$-algebra automorphisms of the image of $\pi$. For any element $c$ of the image of $\pi$, let $tr(c)$ be the sum of the elements $\rho(c)$, $\rho \in H^Z(\mathfrak{m}_0)/HT(\mathfrak{m}_0)$, and notice that, if $c \in B'/\mathfrak{m}_0$, then $tr(c) \in A/m$. If $b \in B'/\mathfrak{m}_0$ and $a \in \overline{A}$, then

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

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, $\bar{A}_p / \mathfrak{p}\bar{A}_p = A'_p / \mathfrak{p}A'_p$, and so $\bar{A}_p / \mathfrak{p}\bar{A}_p$ is a separable $A_p / \mathfrak{p}A_p$-algebra. Thus $\bar{A}$ 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