Pacific Journal of Mathematics

INFINITE GALOIS THEORY FOR COMMUTATIVE RINGS

JOHN E. CRUTHIRDS

Vol. 64, No. 1 May 1976

PACIFIC JOURNAL OF MATHEMATICS
Vol 64, No 1, 1976

INFINITE GALOIS THEORY FOR COMMUTATIVE RINGS

JOHN E. CRUTHIRDS

Let S be a commutative ring with identity. A group G of automorphisms of S is called locally finite, if for each $s \in S$, the set $\{\sigma(s): \sigma \in G\}$ is finite. Let R be the subring of G-invariant elements of S. An R-algebra T is called locally separable if every finite subset of T is contained in an R-separable subalgebra of T. For an R-separable subalgebra T of S and for G a locally finite group of automorphisms it is shown that T is the fixed ring for a group of automorphisms of S. If, in addition, it is assumed that S has finitely many idempotent elements, then it is shown that any locally separable subring T of S is the fixed ring for a locally finite group of automorphisms of S. Examples are included which show the scope of these theorems.

As in **[6]** the closure of G with respect to a G-stable subalgebra E of the Boolean algebra of all idempotent elements of S is the set of all automorphisms ρ of S for which there exist a positive integer n and idempotents $e_i \in E$ and automorphisms $\sigma_i \in G$, such that $\bigcup_{i=1}^{n} e_i = 1$ and $e_i \cdot \rho = e_i \cdot \sigma_i$ for $1 \leqq i \leqq n$. The closure of G with respect to the set of all idempotent elements of S will be called the Boolean closure of G.

1. Infinite Galois theory.

Throughout this section, G will be a locally finite group of automorphisms of a commutative ring S and R will be the subring of G-invariant elements of S. The following definition will be needed in §3.

DEFINITION. A ring S is called a Galois extension of a ring R with Galois group H if H is finite with $R = S^H$, and if there exist a positive integer n and elements x_i, y_i of S, $1 \leqq i \leqq n$, such that $\Sigma_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$ for all $\sigma \in H$.

LEMMA 1.1. *Let G be a locally finite group of automorphisms of S with $R = S^G$. If T is an R-separable subalgebra of S and $H = \{\sigma \in G \mid \sigma|_T = 1_T\}$, then $[G: H] < \infty$.*

Proof. Let $\Sigma_{i=1}^{n} x_i \otimes y_i$ be a separability idempotent for T over R. Then $\Sigma_{i=1}^{n} x_i y_i = 1$, and, for every $t \in T$, $\Sigma_{i=1}^{n} t \cdot x_i \otimes y_i = \Sigma_{i=1}^{n} x_i \otimes y_i t$ in $T \otimes_R T$ **[4]**. Let $K = \{\sigma \in G: \sigma(y_i) = y_i,\ 1 \leqq i \leqq n\}$. Then $H \subseteq K$. But if $\sigma \in K$ and $t \in T$, then

$$\sigma(t) = \left(\sum_{i=1}^{n} x_i y_i\right) \cdot \sigma(t) = \pi \circ (1 \otimes \sigma)\left(\sum_{i=1}^{n} x_i \otimes y_i t\right)$$
$$= \pi \circ (1 \otimes \sigma)\left(\sum_{i=1}^{n} t x_i \otimes y_i\right)$$
$$= \pi\left(\sum_{i=1}^{n} t x_i \otimes y_i\right) = \sum_{i=1}^{n} t x_i y_i = t,$$

where π is the ring multiplication for T. So $\sigma \in H$ and $H = K$. But $K = \bigcap_{i=1}^{n} K_i$ where $K_i = \{\sigma \in G \colon \sigma(y_i) = y_i\}$. Since G is locally finite, $[G \colon K_i] < \infty$ for $1 \leqq i \leqq n$. So K, and hence H, has finite index in G.

THEOREM 1.1. *Let G be locally finite with $R = S^G$ and let T be an R-separable subalgebra of S. Then there is an R-separable subalgebra T' of S containing T which is G-stable. Moreover, G restricts to a finite group of automorphisms of T'.*

Proof. Let $H = \{\sigma \in G \colon \sigma|_T = 1_T\}$. Then by Lemma 1.1 $[G \colon H]$ is finite, i.e., G/H has finitely many elements, say $\sigma_1 H, \cdots, \sigma_k H$. Then $\Pi_{\sigma \in G}\, \sigma(T) = \Pi_{i=1}^{k}\, \sigma_i(T)$. Since T is R-separable, $\sigma(T)$ is R-separable for $\sigma \in G$. Since $\Pi_{i=1}^{k}\, \sigma_i(T)$ is a homomorphic image of the tensor product of the $\sigma_i(T)$, it follows from [**1**, Propositions 1.4, 1.5] that $\Pi_{i=1}^{k}\, \sigma_i(T)$ is an R-separable subalgebra of S. Let $T' = \Pi_{\sigma \in G}\, \sigma(T)$. Then $T \subseteq T'$ and T' is G-stable. The moreover statement follows from Lemma 1.1 applied to T'.

COROLLARY 1.1. *If G is locally finite with $R = S^G$ and T is R-separable, then T is finitely generated and projective as an R-module.*

Proof. By the Theorem $T \subseteq T'$ where T' is R-separable and G restricts to a finite group of automorphisms of T'. The corollary follows from the Theorem of [**6**].

OBSERVATION. Suppose T is an R-separable subalgebra of S and let $s \in S \backslash T$. If S' denotes the subring of S generated by s and T, then S' is generated as an R-algebra by $\{s, t_1, \cdots, t_n\}$ where $t_1, \cdots, t_n$ are the R-module generators of T. So if $\sigma \in G$, $\sigma(S')$ is determined by $\sigma(s), \sigma(t_1), \cdots, \sigma(t_n)$. Since G is locally finite it follows that S' has only finitely many distinct images under G, say $\sigma_1(S'), \cdots, \sigma_l(S')$. Let $T' = \Pi_{\sigma \in G}\, \sigma(S')$. Then $T' = \Pi_{i=1}^{l}\, \sigma_i(S')$ and T' is generated as an R-algebra by $\{\sigma(s), \sigma(t_1), \cdots, \sigma(t_n) \colon \sigma \in G\}$ which is finite since G is locally finite. T' is also G-stable. If $K = \{\sigma \in G \colon \sigma|_{T'} = 1_{T'}\}$, then K is precisely the set of all σ in G which leave every R-algebra generator of T' fixed. Since G is locally finite, this latter group has finite index in G. So G restricts to a finite group of automorphisms of T'. So T' is a G-stable subalgebra of S containing s and T, and G restricts to a finite group on T'.

COROLLARY 1.2. *If G is locally finite with $R = S^G$ and T is an R-separable subalgebra of S, then there is a subgroup H of $\bar{G}$ with $T = S^H$ where $\bar{G}$ denotes the Boolean closure of G.*

Proof. Let $s \in S \backslash T$. By the observation there is a G-stable subalgebra T' of S containing s and T, and $G|_{T'}$ is finite. By the Theorem of **[6]** there is a finite subgroup K of the closure of $G|_{T'}$ with respect to the idempotent elements of T' such that $T = (T')^K$. In particular, there is $\rho \in K$ such that $\rho(s) \neq s$. By Proposition 2 of **[6]** this element ρ of K is of the form $\rho = \sum_{i=1}^n e_i(\sigma_i)|_{T'}$ where $E = \{e_1, \cdots, e_n\}$ is a $G|_{T'}$-stable set of pairwise orthogonal idempotent elements of T' such that $\sum_{i=1}^n e_i = 1$. Since T' is G-stable, it follows from Propositions 1 and 2 of **[6]** that $\sum_{i=1}^n e_i\sigma_i$ is an element of $\bar{G}$. But $(\sum_{i=1}^n e_i\sigma_i)(s) = \rho(s) \neq s$. Since s was any element of $S \backslash T$, it follows that $T = S^H$ for $H = \{\sigma \in \bar{G} \colon \sigma|_T = 1_T\}$.

It should be noted here that none of the preceding results has had any restriction on the number of idempotent elements in the ring S. In Theorem 1.2 below it is assumed that S has only finitely many idempotent elements. Example 2 in §3 of this paper shows that this assumption is needed.

The proof of Theorem 1.2 requires that the Krull topology be placed on $S^S = \mathrm{Map}(S, S)$, the set of single-valued mappings of S into itself. If H is a group of automorphisms of S and f is an element of the closure of H in S^S with respect to the Krull topology and s and t are elements of S, then there is $\sigma \in H$ such that $\sigma(s) = f(s)$, $\sigma(t) = f(t)$, $\sigma(s+t) = f(s+t)$, $\sigma(s \cdot t) = f(s \cdot t)$. Since $\sigma(s+t) = \sigma(s) + \sigma(t)$ and $\sigma(s \cdot t) = \sigma(s) \cdot \sigma(t)$, the same properties hold for f and it follows that f is in fact a ring homomorphism of S. Taking $s \neq t$ in the above argument also shows f is a monomorphism. If H is also locally finite and $y \in S$, then $\{\sigma(y) \mid \sigma \in H\}$ is finite, say $\{\sigma(y) \mid \sigma \in H\} = \{s_1, \cdots, s_n\}$. So there is an element $\sigma \in H$, with $\sigma(s_i) = f(s_i)$, $1 \leqq i \leqq n$. Since $\sigma^{-1} \in H$, there is a j, $1 \leqq j \leqq n$, with $\sigma^{-1}(y) = s_j$. Then $f(s_j) = \sigma(s_j) = y$ and f is an automorphism of S. If $(x_1, \cdots, x_k)$ are any k elements of S, there is $\sigma \in H$ such that $\sigma(f^{-1}(x_i)) = x_i$ because $f(f^{-1}(x_i)) = x_i$, $1 \leqq i \leqq k$. So $f^{-1}(x_i) = \sigma^{-1}(x_i)$, each i, and it follows that f^{-1} is also in the closure of H. It now follows readily that the closure of a locally finite group of automorphisms of S is again a locally finite group of automorphisms of S.

THEOREM 1.2. *Let G be a locally finite group of automorphisms of S with $R = S^G$. Assume S has only finitely many idempotent elements. If T is* *a locally separable R-subalgebra of S, then there is a locally finite group H of automorphisms of S with $T = S^H$.*

Proof. Let $\bar{G}$ be the closure of G with respect to the Boolean algebra of all idempotent elements of S. Since S has only finitely many idempotent elements, $\bar{G}$ is a locally finite group of automorphisms of S. Let $\bar{G}^C$ be the closure of $\bar{G}$ in the Krull topology on S^S. $\bar{G}^C$ is a locally finite group of automorphisms of S, and the usual argument shows that $\bar{G}^C$ is compact. Now take $y \in S \backslash T$. For $t \in T$, let $A_t = \{\sigma \in \bar{G}^C : \sigma(t) = t, \sigma(y) \neq y\}$. Since T is locally separable, Corollary 1.2 can be applied to show that if $t_1, \cdots, t_n$ are any elements of T, then $\bigcap_{i=1}^n A_{t_i} = \{\sigma \in \bar{G}^C : \sigma(t_i) = t_i, 1 \leqq i \leqq n, \sigma(y) \neq y\} \neq \emptyset$. So $\{A_t\}_{t \in T}$ is a collection of closed subsets of $\bar{G}^C$ which have the finite intersection property. Since $\bar{G}^C$ is compact, it follows that $\bigcap_{t \in T} A_t \neq \emptyset$. So there exists $\sigma \in \bar{G}^C$ such that $\sigma|_T = 1_T$ and $\sigma(y) \neq y$. Letting $H = \{\sigma \in \bar{G}^C : \sigma|_T = 1_T\}$, $T = S^H$ and H is locally finite since it is a subgroup of $\bar{G}^C$.

THEOREM 1.3. *Let G be a locally finite group of automorphisms of S with $R = S^G$. Let S be locally separable over R with finitely many idempotents. Then an R-subalgebra T of S is the fixed ring of a locally finite group of automorphisms of S if and only if T is locally separable.*

Proof. The implication one way follows from Theorem 1.2.

Now let H be a locally finite group of automorphisms of S with $T = S^H$. Let $\{t_1, \cdots, t_n\}$ be a finite subset of T. Since S is locally separable, there exists an R-separable subalgebra S' of S such that $\{t_1, \cdots, t_n\} \subseteq S'$. Let $S'' = \Pi_{\sigma \in H} \sigma(S')$ be the subalgebra of S generated by $\{\sigma(S') : \sigma \in H\}$. Then, as in the proof of Theorem 1.1, S'' is an R-separable subalgebra of S, and S'' is clearly H-stable. By Corollary 1.1, S'' is also finitely generated and projective as an R-module. Corollary 1.2 now says that $S'' = S^J$, where $J = \mathrm{Aut}_{S''}(S)$. Proceeding now as in the proof Theorem 1.10(b) of **[9]**, it can be shown that $S'' \cap S^H$ is a separable R-algebra. But $S^H = T$, so $S'' \cap S^H = S'' \cap T \supseteq S' \cap T \supseteq \{t_1, \cdots, t_n\}$. Therefore, T is locally separable.

It has been noted that Theorem 1.2 has the hypothesis that the ring S have only finitely many idempotent elements. This hypothesis was used in the proof of Theorem 1.2 to show that the group $\bar{G}$ was a locally finite group. The following question naturally arises: Is there some weaker condition on S which will still give $\bar{G}$ locally finite? Theorem 1.4, below, answers this question negatively in the case where the ring R has no nontrivial idempotent elements.

In the following, weakly Galois is used as in definition 3.1 of **[11]**, and $\bar{G}$ is the Boolean closure of G.

LEMMA 1.4. *Let S be weakly Galois over R with $R = S^G$ and G a finite group of automorphisms of S. Suppose R is connected, i.e., R has no nontrivial idempotents. Let T be an R-separable subalgebra of S, such that T is $\bar{G}$-stable. Then either T is connected or T contains all the idempotent elements of S.*

Proof. Since $\bar{G}$ is its own Boolean closure in S, it follows by (3.9 d), p. 93 of **[11]** that $\bar{G} = \mathrm{Aut}_R(S)$. So T is normal in the sense of Definition 2.1 of **[9]**, and the lemma follows from Proposition 2.3 of **[9]**.

THEOREM 1.4. *Assume R is connected and let S be a locally separable R-algebra with $R = S^G$, where G is a locally finite group of automorphisms. Then S has finitely many idempotent elements if and only if $\bar{G}$ is locally finite.*

Proof. If S has finitely many idempotent elements, then it is clear that $\bar{G}$ is locally finite since G is locally finite. Conversely, suppose $\bar{G}$ is locally finite. Let e be a nontrivial idempotent element in S. Let T be a separable subalgebra of S containing e. Let $T' = \Pi_{\sigma \in \bar{G}} \sigma(T)$. Then T' is a separable subalgebra of S since $\bar{G}$ is locally finite. Let f be any other idempotent element in S. As with T' above, there is a separable subalgebra U of S containing both T' and f which is also $\bar{G}$-stable. The locally finite group $\bar{G}$ induces a finite group of automorphisms on the separable subalgebra U. So U is weakly Galois over R, and it follows from Lemma 1.4 that T' contains all the idempotent elements in U. In particular, T' contains f. T' then contains all the idempotent elements in S. But since T' is weakly Galois over the connected ring R, T' can contain only finitely many idempotent elements (Theorem 2.1 gives an easy proof of this).

2. Applications to the finite Galois theory. In this section it will be assumed that S is a commutative ring and G is a finite group of automorphisms of S. Since a finite group is clearly locally finite, an attempt will be made to apply some of the results of §1 to the case where G is in fact a finite group. R will again be the subring of G-invariant elements of S. Lemma 2.1, and Theorem 2.1 belong to the author's major professor, H. F. Kreimer, and are included here with his permission. They show that S has finitely many idempotents if, and only if, R has finitely many idempotents.

Note that if p is a prime ideal of R then it follows by [**2**, Ch. 5, §2, Thm. 2] that G acts transitively on the set of prime ideals of S which lie over p. Since G is finite, it can also be concluded that the set of prime ideals of S which lie over a given prime ideal of R is finite.

DEFINITION. A commutative ring will be called semi-local if it has only finitely many maximal ideals.

LEMMA 2.1. *S is semi-local if, and only if, R is semi-local.*

Proof. If M is a maximal ideal of S, then $R \cap M$ is a maximal ideal of R, and if m is a maximal ideal of R, then there exists a maximal ideal of S which lies over m by [**2**, Chapter 5, §2, Prop. 1 and Thm. 1]. So if S is semi-local, R is also. Also, only a finite number of maximal ideals of S can lie over a given maximal ideal of R. So S is semi-local if R is semi-local.

THEOREM 2.1. *S has finitely many idempotent elements if, and only if, R has finitely many idempotent elements.*

Proof. It is clear, of course, that R has finitely many idempotent elements if S does. If E is the Boolean algebra of all idempotent elements of S, then the elements of G restrict to automorphisms of E and the subset of G-invariant elements of E is the Boolean algebra of idempotent elements of R. The theorem is an immediate consequence of Lemma 2.1 and the fact that a Boolean algebra is semi-local if and only if it is finite by Stone's Representation Theorem [**10**, p. 351].

LEMMA 2.2. *If R has finitely many idempotent elements and G is a finite group of automorphisms of S such that $R = S^G$, then there is a unique maximal R-separable subalgebra of S.*

Proof. Since R has only finitely many idempotent elements, S has only finitely many idempotent elements by Theorem 2.1. Let $\bar{G}$ be the closure of G with respect to the Boolean algebra of idempotent elements of S. Then $\bar{G}$ is a finite group. For an R-algebra T such that $R \subseteq T \subseteq S$ and T is separable over R, let $H(T) = \{\sigma \in \bar{G} \colon \sigma|_T = 1_T\}$. By Corollary 1.2, $T = S^{H(T)}$. Pick an R-separable subalgebra T_0 of S such that $H(T_0)$ has smallest order. Let T be any R-separable subalgebra of S. Then $T \cdot T_0$ is a separable subalgebra of S containing T_0, hence $H(T \cdot T_0) \subseteq H(T_0)$. But $|H(T_0)| \leqq |H(T \circ T_0)|$. Therefore, $H(T \cdot T_0) = H(T_0)$ and $T \subseteq T \cdot T_0 = S^{H(T \cdot T_0)} = T_0$. It follows then that T_0 is the unique maximal separable subalgebra of S.

It can be noted here that it is a straightforward Zorn's lemma exercise to show that S always contains a maximal locally separable subalgebra, and this requires no restrictions on the number of idempotent elements of S.

THEOREM 2.2. *If R has finitely many idempotent elements and G is a finite group of automorphisms of S such that $R = S^G$, then every locally separable subalgebra of S is in fact separable over R.*

Proof. S has only finitely many idempotent elements by Theorem 2.1. Lemma 2.2 says that S contains a unique maximal R-separable subalgebra, say T_0. Let T be any locally separable subalgebra of S. If t is any element of T then t is contained in some R-separable subalgebra of T, say T'. But $T' \subseteq T_0$ by the maximality of T_0. So $t \in T_0$ and, hence, $T \subseteq T_0$. Since G is finite and S has only finitely many idempotent elements, Theorem 1.2 can be used to show that there is a finite group H of automorphisms of S with T as fixed ring, i.e., $T = S^H$. Since the image of T_0 under an automorphism of S would be separable, T_0 must be H-stable. So H can be considered as a finite group of automorphisms of T_0 and $T_0^H = S^H = T$. By Theorem 1.1 and Corollary 1.1, T_0 is weakly Galois over R. T is then separable over R by [**11**, 3.10, p. 93].

3. Examples. In this section three examples are given in an attempt to show that the major results of §§1 and 2 are in some sense as sharp as might be hoped for.

EXAMPLE 1. Corollary 1.2 shows that if G is locally finite with $R = S^G$, then a separable intermediate algebra T is the fixed ring for a subgroup H of the closure of G with respect to a certain collection of idempotent elements. This example shows that, in general, G must be enlarged in order to find the group H, even in the rather nice case where S is a Galois extension of R. Rings R, S, T are given such that $R \subseteq T \subseteq S$, S is Galois over R, T is separable over R, and T is not the fixed ring of a subgroup of *any* Galois group for S over R, where a Galois group is a group for which statement (b) of Theorem 1.3 of [**3**] is satisfied.

Let $\mathbf{C}$ be the field of complex numbers and let $\mathbf{R}$ be the field of real numbers. All tensoring here will be done over the ring $\mathbf{R}$. Since $\mathbf{C}$ is a Galois extension of $\mathbf{R}$, $\mathbf{C} \otimes \mathbf{C}$ is a Galois extension of $\mathbf{R}$. A Galois group for $\mathbf{C} \otimes \mathbf{C}$ over $\mathbf{R}$ is $G = \{1 \otimes 1,\ 1 \otimes \sigma,\ \sigma \otimes 1,\ \sigma \otimes \sigma\}$, where σ is conjugation on $\mathbf{C}$. The separability idempotent for $\mathbf{C} \otimes \mathbf{C}$ over $\mathbf{R}$ is $e = \frac{1}{4}(1 \otimes 1 \otimes 1 \otimes 1 - 1 \otimes i \otimes 1 \otimes i - i \otimes 1 \otimes i \otimes 1 + i \otimes i \otimes i \otimes i)$. Let τ be the element of $\mathrm{Aut}_{\mathbf{R}}(\mathbf{C} \otimes \mathbf{C})$ given by $\tau(w \otimes z) = z \otimes w$. If e is viewed as $\Sigma_{i=1}^4 x_i \otimes y_i$, then $\Sigma_{i=1}^4 x_i \tau(y_i) = \frac{1}{2}[1 \otimes 1 - i \otimes i] \neq 0$. So τ can-not be an element of any Galois group for $\mathbf{C} \otimes \mathbf{C}$ over $\mathbf{R}$ by [**3**, Theorem 1.3(b)]. Take S to be $\mathbf{C} \otimes \mathbf{C}$, R to be $\mathbf{R}$, and $T = (\mathbf{C} \otimes \mathbf{C})^{\{1,\tau\}}$. Since T is the fixed ring of a locally finite group of automorphisms of S, T is locally separable over R by Theorem 1.3. But $\mathbf{C} \otimes \mathbf{C}$ has only two nontrivial idempotent elements, namely, $e_1 = \frac{1}{2}(1 \otimes 1 - i \otimes i)$ and $e_2 = \frac{1}{2}(1 \otimes 1 + i \otimes i)$. Therefore, Theorem 2.2 says T is in fact separable over R. By [**3**, Cor. 3.3] every ring endomorphism of the R-algebra S is of the form $\eta = e_1\sigma_1 + e_2\sigma_2$ for $\sigma_1, \sigma_2 \in G$. A direct check shows that the only automorphisms of S over R are $1 \otimes 1$, $1 \otimes \sigma$, $\sigma \otimes 1$, $\sigma \otimes \sigma$, τ, $\tau \circ (1 \otimes \sigma)$, $\tau \circ (\sigma \otimes 1)$, $\tau \circ (\sigma \otimes \sigma)$. It is also easy to show that $1 \otimes 1$ and τ are the only automorphisms which fix $(1+i) \otimes (1+i)$. Thus $\{1 \otimes 1, \tau\}$ is the only group for which T is the subring of invariant elements.

EXAMPLE 2. Theorem 1.2 shows that if the ring S has finitely many idempotent elements and G is locally finite then any locally separable intermediate ring is the fixed ring for a locally finite group of automorphisms of S. This example shows that the restriction that S have only finitely many idempotent elements is needed. Rings R, S, T and a locally finite group G of automorphisms of S are given such that $R = S^G$, $R \subseteq T \subseteq S$, and T is locally separable over R, but T is not left fixed by any nonidentity automorphism of S. In fact, the ring R in this example has no nontrivial idempotent elements. Therefore, it does not even look like a generalized version of Theorem 1.2 without restrictions on the number of idempotents in S could be obtained by reducing to the case where the bottom ring is connected as is done in [**11**].

The example deals with certain sequences of complex numbers under coordinate-wise addition and multiplication. For $i \geqq 0$ and $0 \leqq j < 2^i$ let e_{ij} be the sequence with a one in the entries of the form $j + k \cdot 2^i + 1$ for $k \geqq 0$, and all other entries zero. Then each e_{ij} is an idempotent element and $e_{ij} = e_{i+1,j} + e_{i+1,j+2^i}$, for all i, j.

DEFINITION. Let S be the ring consisting of all the sequences of complex numbers which are finite linear combinations over $\mathbf{C}$ of the e_{ij}.

Let σ_{ij}, $i \geqq 0$ and $0 \leqq j < 2^i$, be the element of $\mathrm{Aut}(S)$ which acts on a sequence by interchanging the $j + k \cdot 2^{i+1} + 1$ and $j + k \cdot 2^{i+1} + 2^i + 1$ entries for $k \geqq 0$. Then $\sigma_{ij}\,(e_{i+1,j}) = e_{i+1,j+2^i}$ and $\sigma_{ij}(e_{ij}) = e_{ij}$. In fact, if $i \leqq k$ then $\sigma_{kl}\,(e_{ij}) = e_{ij}$ for all possible l and j.

DEFINITION. Let G be the subgroup of $\mathrm{Aut}(S)$ generated by the σ_{ij} along with the automorphism τ which acts on a sequence by conjugating every entry in the sequence.

Let $R = S^G$. Then if $(x_m) \in R$, it must be the case that each x_m is a real number since $\tau \in G$. If $n > 1$, let i be the smallest integer such that $n \leqq 2^{i+1}$. Letting $j = n - 2^i - 1$, $n = j + 2^i + 1$ and $0 \leqq j < 2^i$. Then σ_{ij}

interchanges the nth and $(j+1)$st entries of (x_m). Since $j+1<n$, an easy induction argument will show that $x_n = x_1$ for all $n \geqq 1$. Therefore, S^G is exactly the subring of S consisting of all constant sequences of real numbers.

An element $s \in S$ can be written as $s = \sum_{j=0}^{2^i-1} c_j e_{ij}$ with $c_j \in \mathbf{C}$ for sufficiently large i. If $i \leqq k$ then σ_{kl} fixes the e_{ij} and hence s. So the distinct images of s under G are the distinct images of s under the subgroup of G generated by τ and the σ_{kl}, for $k<i$. But if $k<i$, σ_{kl} will map e_{ij} to e_{ip}, some p such that $0 \leqq p < 2^i$. Since there are only finitely many e_{ij}, s can have but a finite number of distinct images under this subgroup of G. So G is a locally finite group of automorphisms of S.

DEFINITION. Let T be the subring of S consisting of all the elements $s \in S$ which have c_{2^i-1} a real number when s is expressed in the form $s = \sum_{j=0}^{2^i-1} c_j e_{ij}$, some $i>0$.

Then T is an ${}^{\bullet}R$-subalgebra of S and T contains all the e_{ij}. Let $t_1, \cdots, t_n$ be elements of T. Fix an integer p so that each t_i, $1 \leqq i \leqq n$, can be written as a linear combination of the e_{pj}, $0 \leqq j \leqq 2^p-1$. The subring of T generated over R by the e_{ij} for $i \leqq p$ is isomorphic to

$$\underbrace{\mathbf{C} \oplus \cdots \oplus \mathbf{C}}_{2^p-1} \oplus \mathbf{R}$$

and hence is separable over R. So T is in fact locally separable over R.

At this stage G is a locally finite group of automorphisms of the ring S, $R = S^G$ has no nontrivial idempotent elements, and T is locally separable over R with $R \subset T \subset S$. That T is not left fixed by any nonidentity automorphism of S follows from the

LEMMA. *If γ is any automorphism of S such that $\gamma|_T = 1_T$, then $\gamma = 1_S$.*

Proof. Let $x \in S$ be arbitrary. Let i be a positive integer. Let p be an integer so that x can be written as $x = \sum_{t=0}^{2^p-1} c_t e_{p,t}$, $c_t \in \mathbf{C}$. Since, in general, $e_{j,2^j-1}$ begins with 2^j-1 zeros, it is possible to choose an integer $q>p$ so that $(e_{q,2^q-1})_i = 0$. View x as a linear combination of the $e_{q,s}$, say $x = \sum_{s=0}^{2^q-1} d_s e_{q,s}$. Then

$$\begin{aligned}(\gamma(x))_i &= \left[\gamma\left(\sum_{s=0}^{2^q-2} d_s \cdot e_{q,s}\right) + \gamma(d_{2^q-1} \cdot e_{q,2^q-1})\right]_i \\ &= \left[\gamma\left(\sum_{s=0}^{2^q-2} d_s \cdot e_{q,s} + 0 \cdot e_{q,2^q-1}\right)\right]_i + [\gamma(d_{2^q-1} \cdot e_{q,2^q-1})]_i \\ &= \left[\sum_{s=0}^{2^q-2} d_s \cdot e_{q,s} + 0 \cdot e_{q,2^q-1}\right]_i + [\gamma(d_{2^q-1} \cdot e_{0,0}) \cdot \gamma(e_{q,2^q-1})]_i .\end{aligned}$$

But $[\sum_{s=0}^{2^q-2} d_s \cdot e_{q,s} + 0 \cdot e_{q,2^q-1}]_i = x_i$ since $(_{q,2^q-1})_i = 0$, and $[\gamma(e_{q,2^q-1})]_i = (e_{q,2^q-1})_i = 0$ since $\gamma\,|_T = 1_T$. It follows then that $(\gamma(x))_i = x_i$. Since x and i were arbitrary, $\gamma = 1_S$.

EXAMPLE 3. Theorem 2.2, shows that,.in the finite case, the assumption of finitely many idempotent elements in R (or S, Theorem 2.1) will give locally separable implies separable. This example shows that, in general, the result fails even in the setting where S is a Galois extension of R. The rings R, S, T are given as follows:

S — all sequences of complex numbers which are eventually constant.

T — all sequences of complex numbers which are eventually a constant real number.

R — all sequences of *real* numbers which are eventually constant.

Let σ be the automorphism of S which acts on a sequence by conjugating each term. Then a group of automorphisms of S with fixed ring R is obtained by considering 1_S and σ. Let $G = \{1_S, \sigma\}$. Let $x_1 = (1, 1, 1, \cdots)$, $x_2 = (i, i, i, \cdots)$, $y_1 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \cdots)$, and $y_2 = (-\frac{i}{2}, -\frac{i}{2}, -\frac{i}{2}, \cdots)$. It is readily verified that $\sum_{i=1}^{2} x_i y_i = (1, 1, 1, \cdots)$ and $\sum_{i=1}^{2} x_i \sigma(y_i) = (0, 0, 0, \cdots)$. It follows then by [**3**, Theorem 1.3(b)] that S is in fact a Galois extension of R, and by [**7**, Example 1] T is not separable over R. It remains to be seen that T is locally separable. Let F be a finite subset of T. Then there is a positive integer N such that if $i, j \geqq N$ and $t \in F$ then $t_i = t_j$, i.e., all the elements of F are constant past the Nth slot. Let T' be the subalgebra of S which consists of all sequences in S which have real entries past the Nth slot. Then $F \subseteq T' \subseteq T$ and $R \subseteq T' \subseteq T$. Let e_i denote the element of S whose ith entry is one and whose other entries are zero, and let f be the element of S given by $f_n = 1$ if $n > N$, $f_n = 0$ otherwise. Then T' is isomorphic to $Se_1 \oplus Se_2 \oplus \cdots \oplus Se_N \oplus Rf$, and it follows that T' is a separable R-algebra because S and R are separable R-algebras. Therefore, T is locally separable over R.

REFERENCES

1. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc., **97** (1960).
2. N. Bourbaki, *Algèbra Commutative*, Hermann, Paris, 1961.
3. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs of Amer. Math. Soc., No. **52** (1965).
4. F. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, Springer-Verlag Lecture Notes in Mathematics, Vol. **181** (1971).
5. N. Jacobson, *Structure of Rings*, Amer. Math. Soc., Colloquium Publications, Vol. **37** (1956).

6. H. F. Kreimer, *Automorphisms of commutative rings*, Trans. Amer. Math. Soc., **203** (1975).
7. ———, *Galois theory and ideals in commutative rings*, Osaka Math. J., **12** (1975).
8. ———, *Outer Galois theory for separable algebras*, Pacific J. Math., **32** (1970).
9. A. R. Magid, *Locally Galois algebras*, Pacific J. Math., **33** (1970).
10. George F. Simmons, *Introduction to Topology and Modern Analysis*, International Series in Pure and Applied Mathematics (1963).
11. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J., **35** (1969).

Received December 16, 1975.

Pacific Journal of Mathematics

Vol. 64, No. 1 May, 1976