GALOIS THEORY FOR RINGS WITH FINITELY MANY IDEMPOTENTS

O. E. VILLAMAYOR and D. ZELINSKY[1]

To the respected memory of Tadashi Nakayama

0. Introduction

In [5], Chase, Harrison and Rosenberg proved the Fundamental Theorem of Galois Theory for commutative ring extensions $S \supset R$ under two hypotheses: (i) S (and hence R) has no idempotents except 0 and 1; and (ii) S is Galois over R with respect to a finite group G—which in the presence of (i) is equivalent to (ii′) : S is separable as an R-algebra, finitely generated and projective as an R-module, and the fixed ring under the group of all R-algebra automorphisms of S is exactly R. We shall refer to the Fundamental Theorem under these hypotheses as "CHR Galois Theory." This terminology is not quite just to Chase, Harrison and Rosenberg, since even if S has idempotents, they have a Fundamental Theorem, but hypothesis (ii) now requires that a finite group G be given (definitely not the group of all automorphisms of S) having R as fixed ring, and satisfying the Galois hypothesis of [2, p. 396]. Furthermore, this Fundamental Theorem gives a one-to-one correspondence between subgroups of this given group and *some* separable subalgebras of S.

In this note, we propose an alternative approach when R (or, rather, the image of R in S) has finitely many idempotents, and when S and R satisfy hypothesis (ii′). These are hypotheses only on S and R and not on a prescribed group of automorphisms (It is true that in this case S is Galois over R with respect to a finite group, in fact, with respect to several different finite groups. It is partly this multiplicity of groups that prompted our investigation). Our conclusions give a one-to-one correspondence between all projective, separable subalgebras of S and some subgroups (called "fat" subgroups) of the full automorphism group of S over R. The fat subgroups are easily describable in

Received August 26, 1965.

[1] This work was supported by NSF grants GP 1649 and GP 3895.

https://doi.org/10.1017/S0027763000026507 Published online by Cambridge University Press

terms of the decomposition of S as direct sum (necessarily finite by Proposition 1.3) of R-algebras. Our approach actually interposes between a subgroup and its associated fixed ring a certain groupoid composed of all the isomorphisms between components of S that can be induced by automorphisms in the subgroup. The standard group-to-algebra correspondence is split into the composite of a many-to-one correspondence from groups of automorphisms to groupoids of isomorphisms, followed by a one-to-one correspondence from groupoids to algebras. The correspondence group $\to$ groupoid is one-to-one exactly on the fat subgroups of the automorphism group.

1. Preliminaries and notations

We are concerned with a homomorphism $R\to S$ of commutative rings with unit and denote by G the group of all R-algebra automorphisms of S. Throughout, S will be *finitely generated and projective as an R-module and separable as an R-algebra.* Separability means that the multiplication map[2] $\mu : S\otimes S\to S$, defined by $\mu(x\otimes y)=xy$, has a one-sided inverse $\nu : S\to S\otimes S$ which is an $(S\otimes S)$-homomorphism (hence also, in the present commutative case, an R-algebra homomorphism) and satisfies $\mu\nu=$ identity. A necessary and sufficient condition for this separability is the existence of an idempotent e $(=\nu(1))$ in $S\otimes S$ with $\mu(e)=1$ and $(x\otimes 1-1\otimes x)e=0$ for all x in S. Such an e is unique.

We remark parenthetically that the hypothesis that S is finitely generated is implied by the projectivity and separability, generalizing [7, Theorem 1]:

PROPOSITION 1.1. *Let S be a separable R-algebra (for this proposition only, S need not be commutative) which is projective as an R-module. Then S is finitely generated as an R-module.*

Proof. As in [4, Ch. VII, Prop. 3.1], let $\{p_i\}\subset S$ and $\{\alpha_i\}\subset \mathrm{Hom}_R(S, R)$ be a projective coordinate system for S over R; i.e., $\sum\alpha_i(x)p_i=x$ for every x in S, $\alpha_i(x)$ being zero for almost all i. Then $\{p_i\otimes 1\}$ and $\{\alpha_i\otimes 1\}$ form a projective coordinate system for the right S-module $S\otimes S$; i.e., $v=\sum(p_i\otimes 1)(\alpha_i\otimes 1)(v)$ for all v in $S\otimes S$. Applying the multiplication map μ, we get $\mu(v)=\sum p_i(\alpha_i\otimes 1)(v)$. Take $v=(x\otimes 1)e$ with x in S and e as above, so that $\mu(v)=x\mu(e)=x$. The sum $\sum p_i(\alpha_i\otimes 1)[(x\otimes 1)e]$ can be taken over a fixed finite

[2] All tensor products are taken over R.

set of indices i, independent of x, because $\{i \mid (\alpha_i \otimes 1)[(x \otimes 1)e] \neq 0\} = \{i \mid (\alpha_i \otimes 1)[(1 \otimes x)e] \neq 0\} = \{i \mid [(\alpha_i \otimes 1)(e)]x \neq 0\} \subset \{i \mid (\alpha_i \otimes 1)(e) \neq 0\}$. If we now write $e = \sum a_j \otimes b_j$ with a_j and b_j in S, we have $x = \sum p_i \alpha_i(xa_j) b_j$, and the finite set $\{p_i b_j\}$ generates S as an R-module.

To return to our general notations, we are concerned with the case where the image of the map $R \to S$ has finitely many idempotents. These induce a corresponding decomposition of S, of G, of all subalgebras of S, and all relevant (especially fat) subgroups of G, thus reducing all our problems to the case where *R has no idempotents except* 0 *and* 1 *and $R \to S$ is a monomorphism.* Henceforth, unless otherwise specified, we shall assume R has this property.

PROPOSITION 1.2. *If a finitely generated projective R-module is a direct sum of R-modules, then the number of summands is not greater than the number of generators.*

[This Proposition also holds if R has idempotents, even infinitely many, if we assume that the summands of the projective module are faithful R-modules, as they must be when $R \to S$ is restricted as above.]

Proof by localization: First assume R is a (not necessarily Noetherian) local ring. The projective module (call it M) is then free, and any decomposition of M will express M as a direct sum of free modules. But the rank of a free module is an invariant, so the number of summands $\leq$ rank of $M \leq$ the cardinal of any generating set. Next, for general R, if $M = \oplus M_\alpha$, then each M_α is finitely generated and projective. If $M_\alpha \neq 0$, then every localization of M_α is nonzero, because the set of prime ideals P of R at which $M_\alpha \otimes R_P = 0$ is an open and closed subset of the connected space Spec R [3, p. 141]. It cannot be all of Spec R, else $M_\alpha = 0$, so it is empty, as desired. We may then use any local ring R_P to conclude that the number of nonzero $M_\alpha =$ number of nonzero $M_\alpha \otimes R_P \leq$ number of generators of $M_\alpha \otimes R_P \leq$ number of generators of M_α [If R has idempotents, the proof needs minor modification to prove that M_α faithful implies $M_\alpha \otimes R_P \neq 0$ for all P.].

PROPOSITION 1.3. *S is a finite direct sum of R-algebras, each of which satisfies the conditions imposed above on S. In addition, each summand has no idempotents except* 0 *and its identity element. If the fixed ring under G is R, then all these summands are isomorphic R-algebras to which* CHR *Galois theory applies. G is* *finite, in fact G is a semidirect product of the symmetric group on the summands of S and the product of the automorphism groups of the summands.*

Proof. Proposition 1.2 implies that S is a finite direct sum of indecomposable R-algebras: $S=\oplus_{i\in I}S_i$ and this decomposition is unique. Indecomposability means that each S_i has no idempotents except 0 and its identity element. Each S_i is automatically finitely generated, projective and separable.

Every automorphism in G must permute the S_i. We assert that if the fixed ring is R, then G is transitive on the S_i, for the sum of the identity elements of all the S_i in one transitivity set (one orbit) is a nonzero idempotent in S which is fixed under the action of G; hence it lies in R, and so must be 1, the sum of the identity elements of *all* the S_i. Thus the transitivity set is the set of all S_i, so that each two S_i's are isomorphic. It is now clear how the group G operates on $S=\oplus S_i$. If G_0 is the normal subgroup leaving every S_i setwise invariant (equivalently, leaving every idempotent of S fixed) then G_0 is the product of the automorphism groups of the S_i, and G/G_0 is isomorphic to the group of all permutations of the set $\{S_i\}$. Since this permutation group is easily realized as a subgroup of G, we have G expressed as a semidirect product. The condition "the fixed ring under G is R" now translates into the condition "the fixed subring of each S_i under its automorphism group is R." Thus CHR Galois theory applies to each S_i; the automorphism group of each S_i over R is finite, and so is G.

The correspondences subgroup→subalgebra and subalgebra→subgroup which we shall use are the usual ones, but we now factor them through groupoids. *We continue to use the notation $S=\oplus_{i\in I}S_i$ for the decomposition of S into indecomposables, and use e_i for the identity element of S_i.*

2. Groups→groupoids→fat groups

A *groupoid* is a category all of whose morphisms are isomorphisms. This concept coincides with older definitions as a set[3] with a composition that is sometimes defined and which satisfies the associative law and the condition that every element has a left and a right identity and inverse [6, p. 132]. To make this connection, of course, the elements of the set are to be the morphisms

[3] We ignore all the complications of set theory; for our purposes, finite groupoids suffice.

or maps in the category. Our notation will be as follows. If h is the groupoid, Ob h denotes the set of objects of h (the set of units in the older version), which *for all our groupoids will be the set* $\{S_i \mid i \in I\}$ *of all the indecomposable summands of* S as in the preceding section. If L and M are in Ob h, the morphisms from L to M (the groupoid elements with L as left unit and M as right unit) will be denoted by $h(L, M)$. In this paper, they will always be R-algebra isomorphisms. In particular, *the groupoid of all isomorphisms of all the* S_i *will be denoted by* g, and the only subgroupoids we shall be concerned with are those whose objects are the same, namely $\{S_i \mid i \in I\}$. Specifically, we make the following association of groups to groupoids and the reverse:

Definition 2.1. If H is a group of automorphisms of S (notation as in § 1), denote by H' the following groupoid:

Ob $H' = \{S_i \mid i \in I\}$

$H'(S_i, S_j) = \{\alpha : S_i \to S_j \mid \alpha$ is the restriction to S_i of some element of $H\}$.

If h is a groupoid of isomorphisms of $\{S_i\}$—always with Ob $h = \{S_i \mid i \in I\}$—define a subgroup h' of G as follows:

$h' = \{\sigma \in G \mid$ for all i, the restriction of σ to S_i is in h—i.e., is an element of $h(S_i, \sigma(S_i))\}$.

Thus $g = G'$ and $G = g'$.

Definition 2.2. A subgroup of G is *fat* if it is of the form h' for some groupoid h. Equivalently, the subgroup H is fat if it contains an automorphism σ whenever the restriction of σ to every S_i coincides with the restriction of an element of H.

Proposition 2.3. $h'' = h$ *for every subgroupoid* h *of* g *with* Ob $h =$ Ob g.

Proof. Clearly $h'' \subset h$. For the reverse inclusion we need only show that every isomorphism α in $h(S_i, S_j)$ is the restriction of some automorphism σ in h'. Such a σ can be defined to be the identity map $S_k \to S_k$ for all $k \neq i, j$; if $i \neq j$, let σ be α^{-1} on S_j; and, of course, $\sigma = \alpha$ on S_i.

Thus we have a one-to-one correspondence between all subgroupoids of g (always with the same objects as g) and all fat subgroups of G. It is also possible to think of the many-to-one correspondence $H \to H'$ from *all* subgroups of G to all subgroupoids of g, which establishes an equivalence relation among the subgroups of G : $H_1 \sim H_2$ if $H_1' = H_2'$. Each equivalence class will contain a unique largest subgroup which will be fat and will equal H'' for every H in the equivalence class.

For our purposes, we need a few trivialities on groupoids.

DEFINITION 2.4. A *component* of a groupoid h is a subset C of Ob h which is maximal with respect to the condition $h(L, M) \neq \emptyset$ for every L, M in C. In other words, C is an equivalence class of elements of Ob h, the equivalence relation being $h(L, M) \neq \emptyset$.

Ob h is then the disjoint union of the components of h.

PROPOSITION 2.5. *$h(L, L)$ is a group.*

Proof. The category axioms supply the associative law and the identity element, and "all morphisms are isomorphisms" supplies the inverse.

PROPOSITION 2.6. *If L, M and N are in the same component of h and $\alpha \in h(L, M)$, then $h(N, M) = \alpha h(N, L)$ and $h(L, N) = h(M, N)\alpha$.*

PROPOSITION 2.7. *Given two groupoids h_1 and h_2 with $h_1 \subset h_2$, they are equal if* (i) *they have the same components, and* (ii) *for each object L, $h_1(L, L) = h_2(L, L)$* (*actually it suffices to demand* (ii) *for one L in each component*).

Proof. (i) asserts that $h_1(L, M)$ is empty if and only if $h_2(M, N)$ is. If they are not empty, pick $\alpha \in h_1(L, M) \subset h_2(L, M)$. By Proposition 2.6 and (ii), $h_1(L, M) = \alpha h_1(L, L) = \alpha h_2(L, L) = h_2(L, M)$.

In category language, we have essentially reduced the structure of every groupoid to that of a set of groups: the groupoid is the disjoint union (coproduct) of the full subcategories determined by the components; and each of these subcategories is the product of a group $h(L, L)$ and a "zero groupoid" whose objects are the objects in the component and which has exactly one morphism between each two objects (every object is initial and final).

3. Groupoids $\leftrightarrow$ Algebras

DEFINITION 3.1. If T is an R-subalgebra of S, the groupoid T^* corresponding to T is defined thus:

$$\text{Ob } T^* = \{S_i \mid i \in I\}, \text{ as always}$$
$$T^*(S_i, S_j) = \{\alpha : S_i \to S_j \mid \text{for all } t \text{ in } T, \text{ if } t = \textstyle\sum t_i,\ t_i \in S_i, \text{ then } \alpha(t_i) = t_j\}.$$

If h is a subgroupoid of g with Ob $h = \{S_i \mid i \in I\}$, the algebra corresponding to h is

$$h^* = \{t \in S \mid t = \sum t_i,\ t_i \in S_i,\ \alpha(t_i) = t_j \text{ for all } \alpha \in h(S_i, S_j)\}.$$

We begin by establishing the fact that the usual group $\rightarrow$ ring correspondence is the composite $H \rightarrow H' \rightarrow H'^*$.

Proposition 3.2. *If H is a subgroup of G and H' is the corresponding groupoid, then H'^* is the set of elements in S fixed under H.*

If T is an R-subalgebra of S, then $T^{*\prime}$ is the subgroup of G consisting of all automorphisms which are the identity on T.

Proof. Write an arbitrary t in S as $\sum t_i$ with $t_i \in S_i$. Since every automorphism σ of S permutes the S_i, $\sigma(t) = \sum \sigma(t_i)$ is also the standard decomposition of $\sigma(t)$, except that $\sigma(t_i)$ is the j^{th} component (for some j) rather than the i^{th}. Thus t is fixed under σ if and only if $\sigma(t_i) = t_j$ for every i and corresponding j. Therefore, t is fixed under H if and only if $t \in h^*$ where h is the groupoid consisting of all restrictions of such σ's to S_i's—i.e., $h = H'$.

The other half of the proposition is similarly direct from the definitions.

We now prove, in several steps, that the correspondences $h \rightarrow h^*$ and $T \rightarrow T^*$ establish a one-to-one correspondence.

1. *If $\{S_i \mid i \in J\}$ is a component of h and if e_i is the identity element of S_i, then $\sum_{i \in J} e_i$ is a minimal idempotent in h^*. All the minimal idempotents of h^* are found this way. Thus the components of h are determined by h^*.*

Proof. S_i and S_j are in the same component if and only if $h(S_i, S_j) \neq \emptyset$, which is the same as the existence of an element of h sending e_i to e_j. Thus $\sum_{i \in J} e_i$ is in h^* and no shorter sum will be in h^*. Since the e_i are the only minimal idempotents in S, this shows that $\sum_{i \in J} e_i$ is a minimal idempotent in h^*. Since the union of all the components is the set of all S_i, the sum of these minimal idempotents is 1, proving that we have found them all.

2. *$h(S_i, S_i)$ is the group of all R-algebra automorphisms of S_i which are the identity on the subring $e_i h^*$. Thus $h(S_i, S_i)$ is determined by h^*.*

Proof. $h(S_i, S_i)$ is contained in the group of all automorphisms of S_i over $e_i h^*$ by the definition of h^*. The reverse inclusion follows from CHR Galois

https://doi.org/10.1017/S0027763000026507 Published online by Cambridge University Press

theory applied to the ring S_i, which has no idempotents except 0 and its identity element, e_i.

3. $h = h^{**}$.

Proof. As in the classical case, $h \subset h^{**}$ and $h^* = h^{***}$ so that h and h^{**} are groupoids with the same associated ring h^*. Thus 1., 2., and Proposition 2.7 imply 3.

4. *h^* is finitely generated, projective and separable*[4] *over R.*

Proof. We have already shown in 1. that if $e_J = \sum_{i \in J} e_i$ is the minimal idempotent of h^* corresponding to the component $\{S_i \mid i \in J\}$ of h, then $h^* = \oplus_J e_J h^*$ (because $\sum_J e_J = 1$). So it suffices to show that $e_J h^*$ is finitely generated, projective and separable over R.

Fix one S_0 in the component $\{S_i \mid i \in J\}$ and one isomorphism $\alpha_i : S \to S_i$ in $h(S_0, S_i)$ for each i in J. Since the images of the α_i are orthogonal to each other, $\Theta = \sum \alpha_i$ is an algebra isomorphism of S_0 to a subalgebra T of S, except that Θ maps the identity element of S_0 to e_J, which is the identity element of T but not of S. We can locate $e_J h^*$ as a subalgebra of T thus: $t \in e_J h^*$ if and only if $t = \sum_{i \in J} t_i$ with $t_i \in S_i$ and $\beta(t_i) = t_j$ for all β in $h(S_i, S_j)$. In particular, if $\beta = \alpha_j \alpha_i^{-1}$, we have $\alpha_j^{-1}(t_j) = \alpha_i^{-1}(t_i)$ for all i and j in J; if t_0 denotes this element of S_0, we have $t = \Theta(t_0)$ so that $e_J h^* \subset T$. Similarly, we translate the whole defining property of $e_J h^*$ above to a condition on the subalgebra $\Theta^{-1}(e_J h^*)$ of S_0 by using Proposition 2.6 to get $h(S_i, S_j) = \alpha_j h(S_0, S_0) \alpha_i^{-1}$. Then $t \in e_J h^*$ if and only if $\alpha_j h(S_0, S_0) \alpha_i^{-1}(t_i) = t_j$, i.e., $h(S_0, S_0)(t_0) = t_0$. This means that $\Theta^{-1}(e_J h^*)$ is the fixed subring of S_0 under the group $h(S_0, S_0)$. By CHR Galois theory applied to S_0 and R with group $g(S_0, S_0)$, the fixed ring under a subgroup $h(S_0, S_0)$ is finitely generated, projective and separable. Hence $e_J h^* = \Theta$(fixed ring) has the same properties.

For the other end of the one-to-one correspondence we start with a subalgebra T of S which is finitely generated and projective as an R-module and separable as an R-algebra—as we must, by 4. Here, however, it suffices to assume T is separable over R. This will imply that T is a direct summand in S: By [4, Ch. IX, Prop. 2.2] there is a natural equivalence of functors $\mathrm{Hom}_{T \otimes T}(T, \mathrm{Hom}_R(S, .)) \to \mathrm{Hom}_T(S, .)$ so that if T is $(T \otimes T)$-projective

[4] As in Proposition 1.1, "separable and projective" implies "finitely generated."

and S is R-projective, $\mathrm{Hom}_T(S, .)$ is exact and so S is T-projective; the localization argument in [1, Lemma 4.7] then shows S/T is flat and finitely presented as a T-module, hence projective. Thus $S = T \oplus U$ as T-module. Then T is finitely generated and projective over R because S is.

The argument at the beginning of section 1 gives us an idempotent in $T \otimes_R T$, which we then map to an idempotent, e_T, in $S \otimes_R S$ by the inclusion $T \otimes_R T \to S \otimes_R S$.

5. $T = \{x \in S \mid (x \otimes 1 - 1 \otimes x) e_T = 0\}$, *so that* T *is determined by* e_T.

Proof. Each element of t satisfies the given equation, by definition of the idempotent e_T. For the inverse inclusion, write $S = T \oplus U$ as above. Then $S \otimes S$ is the direct sum of four $(T \otimes T)$-modules, $T \otimes T$, $T \otimes U$, $U \otimes T$, and $U \otimes U$. Since $e_T \in T \otimes T$, an element of $S \otimes S$ is annihilated by e_T only if each of its four components is annihilated by e_T. Write any x in S as $t + u$ with $t \in T$, $u \in U$. Then $x \otimes 1 - 1 \otimes x$ decomposes as the sum of $t \otimes 1 - 1 \otimes t$ which is in $T \otimes T$, and of $u \otimes 1$ in $U \otimes T$ and $-1 \otimes u$ in $T \otimes U$. If $(x \otimes 1 - 1 \otimes x) e_T = 0$ then $e_t(u \otimes 1) = 0$. Apply the multiplication map $\mu : S \otimes S \to S$ and recall that $\mu(e_T) = 1$ by the definition of e_T. This gives $\mu(u \otimes 1) = u = 0$, so that $x \in T$.

We now locate all the idempotents of $S \otimes S$. They are all uniquely sums of minimal idempotents. Since $S \otimes S$ is the direct sum of the rings, $S_i \otimes S_j$, it suffices to find the minimal idempotents of each $S_i \otimes S_j$.

6. *The minimal idempotents in* $S \otimes S$ *are in one-to-one correspondence with the elements of* g. *The minimal idempotents in* $S_i \otimes S_j$ *are in one-to-one correspondence with the isomorphisms* $\alpha : S_i \to S_j$, *i.e., with the elements of* $g(S_i, S_j)$. *The idempotent* e_α *corresponding to* α *has the property*

$$e_\alpha(x \otimes 1) = e_\alpha(1 \otimes \alpha(x)) \text{ for all } x \in S_i.$$

Moreover, the mapping $x \to e_\alpha(x \otimes 1)$ *is an isomorphism of* S_i *to* $e_\alpha(S_i \otimes S_j)$ *and* $y \to e_\alpha(1 \otimes y)$ *is an isomorphism of* S_j *to* $e_\alpha(S_i \otimes S_j)$.

Proof. These e_α are constructed much as Chase, Harrison and Rosenberg did. First, take the unique idempotent e_i' in $S_i \otimes S_i$, as at the beginning of section 1, having the properties $\mu(e_i') =$ the identity element e_i of S_i and

$$e_i'(x \otimes 1 - 1 \otimes x) = 0 \text{ for all } x \text{ in } S_i.$$

Since S_i has no idempotents and μ sends $e_i'(S_i \otimes S_i)$ isomorphically to S_i, it follows that e_i' is a minimal idempotent in $S_i \otimes S_i$. Then for any isomorphism $\alpha : S_i \to S_j$, define

$$e_\alpha = (1 \otimes \alpha)(e_i').$$

This will be a minimal idempotent in $S_i \otimes S_j$, having the property

$$e_\alpha(x \otimes 1 - 1 \otimes \alpha(x)) = (1 \otimes \alpha)[e_i'(x \otimes 1 - 1 \otimes x)] = 0$$

for all x in S_i. Since $x \to e_i'(x \otimes 1)$ is an isomorphism (inverse of μ) of S_i to $e_i'(S_i \otimes S_i)$, apply $1 \otimes \alpha$ to get an isomorphism $x \to e_\alpha(x \otimes 1)$ from S_i to $e_\alpha(S_i \otimes S_j)$. Write $y = \alpha(x)$ and get an isomorphism $y \to x \to e_\alpha(x \otimes 1) = e_\alpha(1 \otimes y)$ from S_j to $e_\alpha(S_i \otimes S_j)$.

These e_α are distinct minimal idempotents and hence orthogonal. Hence to show that the e_α, $\alpha \in g(S_i, S_j)$, are all the minimal idempotents of $S_i \otimes S_j$, it suffices to show that $\sum_\alpha e_\alpha$ is the identity element of $S_i \otimes S_j$. When $i = j$, $\sum_\alpha e_\alpha$ is an element of $S_i \otimes S_i$ fixed under all $1 \otimes \alpha$, α ranging over the R-automorphisms of S_i. But the fixed subring of $S_i \otimes S_i$ under these $1 \otimes \alpha$ is just $S_i \otimes R$ (this is clear if S_i is free over R, and is then true in general by a localization argument). Since $S_i \otimes R \cong S_i$, it has no idempotents, and so $\sum_\alpha e_\alpha$ is the identity element, $e_i \otimes e_i$ of $S_i \otimes S_i$. When $i \neq j$, take one, fixed isomorphism $\alpha : S_i \to S_j$. We just proved that, as β ranges over $g(S_i, S_i)$, $\sum_\beta e_\beta = e_i \otimes e_i$. Since $(1 \otimes \alpha)e_\beta = e_{\alpha\beta}$ and $(1 \otimes \alpha)(e_i \otimes e_i) = e_i \otimes e_j$, we have $\sum_\beta e_{\alpha\beta} = (1 \otimes \alpha)\sum_\beta e_\beta = e_i \otimes e_j$, which is the identity element of $S_i \otimes S_j$. But $\{\alpha\beta \mid \beta \in g(S_i, S_i)\} = g(S_i, S_j)$ by Proposition 2.6.

7. *The idempotent e_T in 5. is exactly $\sum_{\alpha \in T^*} e_\alpha$. Thus e_T, and hence T, are determined by T^*.*

Proof. e_T is expressible as a sum of minimal idempotents e_α. We must show that e_α occurs in this sum (write $e_\alpha < e_T$) if and only if $\alpha \in T^*$. Suppose $e_\alpha < e_T$, $\alpha \in g(S_i, S_j)$ and $x = \sum x_i \in T$ with $x_i \in S_i$. Since the e_α's give a direct sum decomposition the condition $(x \otimes 1 - 1 \otimes x)e_T = 0$ in 5. implies $(x \otimes 1 - 1 \otimes x)e_\alpha = 0$. Now, $e_\alpha \in S_i \otimes S_j$ and so is unchanged by multiplication by $e_i \otimes e_j$. Then from the remark above and from 6.,

$$\begin{aligned} 0 &= (x \otimes 1 - 1 \otimes x) e_\alpha = (x \otimes 1 - 1 \otimes x)(e_i \otimes e_j) e_\alpha \\ &= (x_i \otimes 1 - 1 \otimes x_j) e_\alpha = (1 \otimes \alpha(x_i) - 1 \otimes x_j) e_\alpha. \end{aligned}$$

Using the last isomorphism $y \to e_\alpha(1 \otimes y)$ in 6., we get $\alpha(x_i) = x_j$. This forces

$\alpha \in T^*$.

For the converse, we claim first that for each i there is some $\beta \in T^*(S_i, S_i)$ with $e_\beta < e_T$. Otherwise $e_i \otimes e_i$ annihilates every $e_\alpha < e_T$ and so $(e_i \otimes e_i)e_T = 0$. Applying the multiplication map $\mu : S \otimes S \to S$, we get $0 = e_i^2 \mu(e_T) = e_i$, a contradiction.

Now every $\alpha \in T^*(S_i, S_j)$ can be extended to an automorphism σ of S as in the proof of 2.3. If $x = \sum x_i$ is the decomposition of an element of T with $x_i \in S_i$, this special σ merely interchanges x_i and x_j, leaving the other terms alone. Thus σ is the identity on T, and, since $e_T \in T \otimes T$, $(1 \otimes \sigma)e_T = e_T$. This means that $1 \otimes \sigma$ permutes the minimal idempotents in e_T. But it carries e_β to $e_{\alpha\beta}$, and, since $e_\beta < e_T$, we have $e_{\alpha\beta} < e_T$ for every $\alpha \in T^*(S_i, S_j)$. By Proposition 2.6, the set of all such $\alpha\beta$ is exactly $T^*(S_i, S_j)$. This completes the proof of 7. and hence of the following theorem.

THEOREM. *The correspondences $h \to h^*$ and $T \to T^*$ establish a one-to-one correspondence between all separable R-subalgebras T of S and all groupoids h of isomorphisms of the indecomposable summands S_i of S (as always, we assume* Ob *h is the set of all S_i). The composite correspondence $H \to H'^*$, $T \to T^{*\prime}$ is the usual correspondence between groups and fixed rings, and gives a one-to-one correspondence between all separable R-subalgebras T of S and all fat groups H of automorphisms of S over R.*

REFERENCES

[1] M. Auslander and D. Buchsbaum, *Ramification theory in Noetherian rings*, Am. J. Math., **81** (1959), 749–765.

[2] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc., **97** (1960), 367–409.

[3] N. Bourbaki, *Algèbre Commutative* Ch. 1 and 2, Actualité, Sci. et Ind., no. 1290, Hermann, Paris 1961.

[4] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, N. J., 1956.

[5] S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs of the American Mathematical Society, no. 52, 1965.

[6] N. Jacobson, *Theory of Rings*, Mathematical Surveys, no. 2, Amer. Math. Soc. Publ., New York.

[7] A. Rosenberg and D. Zelinsky, *Cohomology of infinite algebras*, Trans. Amer. Math. Soc., **82** (1956), 85–98.

Universidad de Buenos Aires

Northwestern University