O.E. Villamayor and D. Zelinsky
Nagoya Math. J.
Vol. 35 (1969), 83–98

GALOIS THEORY WITH INFINITELY MANY IDEMPOTENTS[1)]

O.E. VILLAMAYOR AND D. ZELINSKY

1. Introduction.

In 1942 Artin proved the linear independence, over a field S, of distinct automorphism of S; in other words if G is a finite group of automorphisms of S and R is the fixed field, then $\mathrm{Hom}_R(S, S)$ is a free S-module with G as basis. Since then, this last condition ("S is G-Galois") or its equivalents have been used as a postulate in all the Galois theories of rings that are not fields, for example by Dieudonné, Jacobson, Azumaya and Nakayama for noncommutative rings and then in [*AG*, Appendix] and [*CHR*] for commutative rings. When S has no idempotents but 0 and 1, [*CHR*] proves that the ordinary fundamental theorem of Galois theory holds with no real change from the classical, field case.

If the rings have finitely many idempotents, the G-Galois condition prevents the "Galois group" G from being the full automorphism group, but [*CHR*] provides a Galois theory pairing all subgroups of G with certain separable subalgebras. In a sense this is a study of the group G as a transformation group on a commutative ring S. In [*VZ*] we presented a different Galois theory, oriented toward the rings rather than the groups, pairing all separable R-subalgebras of S with some subgroups of the full automorphism group of S over R. The present paper contains the same Galois theory, with no hypotheses at all on idempotents. The technique uses Pierce's representation [*P*] of the ground ring R as the global cross sections of a sheaf of rings that have no nontrivial idempotents, so that at each point x of the base space we have a ring extension of R_x to which [*VZ*] applies.

In order to carry out this program, the G-Galois condition is too restrictive. Our hypothesis, besides the natural finite generation, projectivity,

Received July 13, 1968

1) This research was made possible by N.S.F. Grant GP–1649, Travel Grant GP–8231, and the Conference on Rings and Modules at Oberwolfach, March 1968.

and separability of S over R, can be phrased in three equivalent ways: R is the fixed ring of some finite set (equivalently, group) of automorphisms of S; the S-module $\mathrm{Hom}_R(S,S)$ is generated (not necessarily freely) by automorphisms of S; R is a finite product ΠR_i of rings such that the corresponding direct factor of S is G-Galois over R_i for each i. The last hypothesis was called to our attention by H. F. Kreimer after this manuscript was prepared; he used it to prove theorems similar to ours [K]. Using our techniques, we have appended a proof that it is equivalent to the other two, at the end of section 3.

2. The Boolean spectrum.

Pierce [P] defined, for each commutative ring R, a sheaf of rings $\mathscr{R}$ over a totally disconnected compact Hausdorff space X in such a way that R is the ring of global cross sections of $\mathscr{R}$. We recast his definition slightly in the next few pages. Let $B(R)$ = the Boolean ring consisting of all idempotents of R.

(2. 1) DEFINITION. The *Boolean spectrum* of R is the Stone space $X = \mathrm{Spec}\ B(R)$ consisting of all prime (equivalently, for Boolean rings, maximal) ideals of $B(R)$.

It is possible to describe X without reference to $B(R)$:

(2. 2) A point x in X is a collection of idempotents in R with the properties

(2. 2a) For every idempotent e in R, either $e \in x$ or $1 - e \in x$ but not both;

(2. 2b) If e and f are idempotents in R, then $ef \in x$ if and only if $e \in x$ or $f \in x$.

For each element e in x, there is a neighborhood of x, namely $U_e = \{y \in X \mid e \in y\}$. These neighborhoods form a base of the open sets. Notice $U_e \subset U_f$ if and only if $e \geq f$, that is $ef = f$.

From this description, we deduce a continuous map

(2. 3) ϕ: Spec $R \to X$, $\phi(p)$ = the set of idempotents in p.

Since p is a prime ideal in R and since $e(1-e) = 0$, it is clear that $\phi(p)$ satisfies (2. 2a) and (2. 2b), and so is a point of X. Since $\phi^{-1}(U_e) = \{p \in \mathrm{Spec}\ R \mid e \in p\} = \{p \in \mathrm{Spec}\ R \mid 1 - e \notin p\}$ and this is a basic open set, ϕ is continuous.

https://doi.org/10.1017/S0027763000013039 Published online by Cambridge University Press

Note that $0 \in x$ and $1 \notin x$, for otherwise (2. 2a) implies $0 \notin x$ and $1 \in x$ and (2. 2b) then implies the contradiction $0 = 1 \cdot 0 \in x$. From this and (2. 8) below, we deduce that the R-ideal Rx generated by x is proper for each x (if $1 \in Rx$ then $1 = re$ for some $e \in x$ and $1(1 - e) = 0$, $1 = e \in x$ contradicting the definition of x), hence contained in some maximal ideal p of R. Thus $\phi(p) = x$ and ϕ is surjective.

The following is another version of X which, however, we shall not use explicitly.

(2. 4) *X is homeomorphic to the identification space one gets from Spec R by identifying each connected component to a point. The homeomorphism is induced by ϕ.*

Proof. We first show that, for each $x \in X$, $\phi^{-1}(x)$ is a connected component of Spec R. If V is any connected set in Spec R, $\phi(V)$ is connected in the totally disconnected space X, and hence is a single point. This means that $\phi^{-1}(x)$ is a union of connected components. We need only show $\phi^{-1}(x)$ is connected. The homomorphism $R \to R_x = R/Rx$ induces a continuous map Spec $R_x \to$ Spec R which merely associates to each prime ideal in R_x its inverse image in R. From the definition of ϕ, we see that the image of this map is $\phi^{-1}(x)$. Since Spec R_x is connected (2. 13), so is $\phi^{-1}(x)$.

This shows that X is in one-to-one correspondence with the identification space. To show that the topology of these two spaces agree, we need to show that ϕ is continuous and closed. Its continuity has already been mentioned. Now assume C is closed in Spec R. Then $C = \{p \mid p \supset I\}$ for some ideal I in R. We see that $\phi(C) = \{x \in X \mid$ for some p in Spec R, $p \supset Rx + I\} = \{x \mid Rx + I \neq R\}$. The complement of $\phi(C)$ is $\{x \mid Rx + I = R\}$ and this is open, because $Rx + I = R$ means $re + i = 1$ for some r, e and i in R, x and I respectively (see (2. 8)); but then this same equation says $Ry + I = R$ for every y containing e, and this set of y's is a neighborhood of x.

Pierce's sheaf $\mathscr{R}$ over X is then the direct image, under ϕ, of the standard sheaf $\mathscr{O}(R)$ of local rings over Spec R. In other words, for every open set U in X, the ring of cross-sections of R over U is defined to be $\Gamma(\phi^{-1}(U), \mathscr{O}(R))$, where Γ is the usual cross-section functor. In particular, we computed $\phi^{-1}(U_e)$ above; $\Gamma(U_e, \mathscr{R})$ is the ring of fractions $S^{-1}R$ where S is the multiplicatively closed set generated by $1 - e$. Since $1 - e$ is idempotent, we have

(2. 5) $$\Gamma(U_e, \mathscr{R}) = \{(1-e)\}^{-1}R = R/Re.$$

In particular, if $e = 0$, we get $\Gamma(X, \mathscr{R}) = R$, [P, 4. 4].

We can also describe the single stalks of $\mathscr{R}$ as both rings of fractions of R and homomorphic images of R: For each point x in X, $R_x = \varinjlim \Gamma(U, \mathscr{R})$, the direct limit taken over the directed set of neighborhoods U of x. Using the formula (2. 5), we quickly get

(2. 6) $$R_x = S^{-1}R \text{ where } S = \{1-e \mid e \in x\}$$
$$= R/Rx$$

where, of course, Rx is the ideal of R generated by the elements of x. Note that R_x is flat over R.

In fact, Pierce works even with noncommutative rings. The same remarks we have just made will also apply to this case, substituting the spectrum of the center of R for Spec R.

We need repeatedly the usual sheaf property: if two cross sections agree at a point, then they agree in a neighborhood of the point. However, for the sheaf $\mathscr{R}$ this is easily translated into simple algebraic terms and is quite special. We make this translation now and collect the major applications that we shall need.

DEFINITION. Let M be any R-module. Then

$$M_x = M \otimes_R R_x = S^{-1}M \text{ where } S = \{1-e \mid e \in x\}$$
$$= M/Mx$$

If $a \in M$, then a_x will denote the image of a under $M \to M_x$. We remark that, if M is finitely generated (resp. finitely presented, resp. faithful, resp. projective) as an R-module, then M_x has the same property as an R_x-module. And if M is a separable R-algebra, then M_x is a separable R_x-algebra.

If $g \in \mathrm{Hom}_R(M, M)$, we shall use g_x to denote the R_x-module endomorphism of M_x induced by g. This conflicts with the notation already introduced which would make g_x an element of $\mathrm{Hom}_R(M, M)_x = \mathrm{Hom}_R(M, M) \otimes_R R_x$. We shall adhere to the first version of g_x; in all our cases there is no real conflict, because $\mathrm{Hom}_R(M, M)_x$ will be identified with a subset of $\mathrm{Hom}_{R_x}(M, M)_x$. This is elucidated in the following proposition.

https://doi.org/10.1017/S0027763000013039 Published online by Cambridge University Press

(2. 7) *The map* $g \to g_x$ *from* $\mathrm{Hom}_R(M, M)$ *to* $\mathrm{Hom}_{R_x}(M_x, M_x)$ *is the composite* $\mathrm{Hom}_R(M, M) \to \mathrm{Hom}_R(M, M) \otimes_R R_x = \mathrm{Hom}_R(M, M)_x \to \mathrm{Hom}_{R_x}(M_x, M_x)$; *this last map is a monomorphism when* M *is finitely generated and is an isomorphism when* M *is finitely generated and projective.*

Proof. If F is free on a finite number of generators and $F \to M$ is an epimorphism, then we have induced monomorphisms

$$\mathrm{Hom}_R(M, M) \to \mathrm{Hom}_R(F, M)$$
$$\mathrm{Hom}_R(M, M) \otimes_R R_x \to \mathrm{Hom}_R(F, M) \otimes R_x$$

(since R_x is flat) and isomorphisms

$$\mathrm{Hom}_R(F, M) \otimes_R R_x \cong \mathrm{Hom}_R(F, M_x) \cong \mathrm{Hom}_{R_x}(F_x, M_x)$$

the first resulting from the fact that F is a finite product of R's. Similarly, $F_x \to M_x$ is an epimorphism and induces a monomorphism $\mathrm{Hom}_{R_x}(M_x, M_x) \to \mathrm{Hom}_{R_x}(F_x, M_x)$. Thus in the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(M, M) \otimes_R R_x & \to & \mathrm{Hom}_R(F, M) \otimes_R R_x \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{R_x}(M_x, M_x) & \to & \mathrm{Hom}_{R_x}(F_x, M_x) \end{array}$$

three of the four arrows are monomorphisms. It follows that the fourth is, too. The isomorphism statement is standard [*CE*, VI. 4. 1. 3].

(2. 8) *Every finite set of elements in* Mx *is contained in* Me *for some* $e \in x$. *If* $m_x = 0$ *for all* m *in a finite subset of* M, *then* $m(1 - e) = 0$ *for some* $e \in x$ *and for all* m *in this subset.*

Proof. Such a finite set is contained in $\sum Me_i$ for some finite subset $\{e_i\} \subset x$. If e is the union of the e_i, then $e \in x$ and $e_i \in Re$ so $\sum Me_i \subset Me$ (cf. [P, 1. 6]). The last part of (2. 8) merely asserts $Me(1 - e) = 0$.

(2. 9) *Let* a *and* b *be elements of* M *and* $a_x = b_x$ *at one point of* X. *Then* $a_y = b_y$ *for all* y *in some neighborhood* U_e *of* x, *that is,* $a(1 - e) = b(1 - e)$ *for some* $e \in x$. *If* $a_x = b_x$ *for every* x, *then* $a = b$.

Proof. If $a_x = b_x$ then (2. 8) shows $(a - b)(1 - e) = 0$. If $a_x = b_x$ for every x in X then for each x in X we have $e \in x$ with $a(1 - e) = b(1 - e)$. Since X is compact, it is covered by a finite number of the U_e, say

$U_{e_1}, \cdots, U_{e_n}$. By (2. 10) this means $1 = \sum r_i(1 - e_i)$ so that $a = \sum ar_i(1 - e_i) = \sum br_i(1 - e_i) = b$.

(2. 10) $\cup_{e \in A} U_e = X$ *implies* $1 \in \sum_{e \in A} R(1 - e)$.

Proof. The hypothesis means every x is in some U_e, that is every x meets A, that is, the Boolean ideal generated by all $1 - e$ with $e \in A$ is not contained in any x. This must then be the unit ideal, so that 1 is a linear combination in $B(R)$ of $\{1 - e \mid e \in A\}$. Such a linear combination is also a linear combination in R (the Boolean sum $e \oplus f$ is $e + f - ef$), proving (2. 10).

(2. 11) *If N is a submodule of M and $N_x = M_x$ for all x (note: since R_x is flat over R, $N_x \subset M_x$), then $N = M$ (that is, $\oplus_{x \in X} R_x$ is faithfully flat).*

If M is finitely generated and $N_x = M_x$ for one x, then there is a neighborhood of x such that $N_y = M_y$ for every y in the neighborhood.

Proof. By reducing to M/N, we can assume $N = 0$. If $a \in M$ and $a_x = 0$ then $a \in Mx$. If M is finitely generated, (2. 8) gives $e \in x$ such that $M = Me$. Then for every y containing e, $M_y = 0$. If $a_x = 0$ for all x, then $a = 0$ by (2. 9).

We can lift idempotents:

(2. 12) *Let S be any R-algebra and u any idempotent in S_x. Then there is an idempotent v in S such that $v_x = u$.*

Proof. Lift u to any element w in S. Then $(w^2 - w)_x = 0$. By (2. 9), $(w^2 - w)(1 - e) = 0$ for some $e \in x$. This implies $v = w(1 - e)$ is idempotent and $v_x = w_x - w_x e_x = w_x = u$.

(2. 13) [P, 4. 4] *R_x has no idempotents except* 0 *and* 1.

Proof. If u is idempotent in R_x and v is an extension to R as in (2. 12) then either $v \in x$ or $1 - v \in x$, by (2. 2a). Thus $u = 0$ or 1.

We can extend automorphisms:

(2. 14) *Suppose S is an R-algebra that is finitely presented as an R-module, let N be a finite subset of S and let g be an R_x-algebra automorphism of S_x that is the identity on N_x. Then there is an R-algebra automorphism h of S such that h is the identity on N and $h_x = g$.*

Proof. Let $e_1, \cdots, e_n$ be R-module generators of S whose relations are also finitely generated and let $\sum_j r_{pj}e_j = 0$ be a finite set of defining relations. Further, let $e_ie_j = \sum_k r'_{ijk}e_k$ be the multiplication table of the e's, and let $n_q = \sum_j r''_{qj}e_j$ be the elements of N. Then we are only required to find $f_1, \cdots, f_n$ in S, to serve as $h(e_1), \cdots, h(e_n)$, satisfying

$$\begin{aligned} &\sum_j r_{pj}f_j = 0 \\ &f_if_j - \sum_k r'_{ijk}f_k = 0 \\ &\sum_j r''_{qj}f_j - \sum_j r''_{qj}e_j = 0. \end{aligned} \tag{2. 15}$$

We know this finite set of equations is satisfied modulo Sx by $\{g(e_{ix})\}$. Lift each $g(e_{ix})$ to any element f_i' in S and consider the finite number of elements of S that are the left hand sides of (2. 15) with f_i' replacing f_i. Since these elements are 0 at x, they are all contained in Se for some e in x by (2. 8). It follows that $(f_i')_y$ satisfies (2. 15) for every y in X that contains e. Let $f_i = f_i'(1 - e) + e_ie$. Then for every y in X, either $e \in y$ in which case $f_{iy} = (f_i')_y$ satisfies (2. 15), or $1 - e \in y$ in which case $f_{iy} = e_{iy}$, which also satisfies (2. 15). Thus with these f_i, the left hand sides of (2. 15) are zero at every point of X, hence are zero (2. 9).

(2. 16) THEOREM. *Let S be an R-algebra, finitely generated as an R-module and assume that the group of all R_x-algebra automorphisms of S_x is finite, for each x in X. Then every finite set of R-algebra automorphisms of S generates a finite group (the automorphism group of S is "locally finite").*

Proof. Let $h_1, \cdots, h_n$ be the finite set of automorphisms of S, and H the group they generate. Then for each x, $h_{1x}, \cdots, h_{nx}$ satisfy enough relations to make H_x a finite group. Let m_i be these relations, that is, each m_i is a monomial in the h_j and the h_j^{-1} and $m_i(h_{1x}, \cdots, h_{nx}) = 1$. This last means that the image of each $m_i(h_1, \cdots, h_n)$ under the map $\mathrm{Hom}_R(S, S) \to \mathrm{Hom}_{R_x}(S_x, S_x)$ is the identity. By (2. 7) so is the image in $\mathrm{Hom}_R(S, S) \otimes R_x$. Therefore $m_i(h_1, \cdots, h_n)_x = 1_x$. By (2. 8) with $M = \mathrm{Hom}_R(S, S)$, we have $m_i(h_1, \cdots, h_n)(1 - e) = 1 - e$ for some e in x. Since the h_j are all the identity on e, this means that the h_j induce on S/Se automorphisms that satisfy enough relations (namely the m_i) to generate a finite group. For every x in X, we have produced a neighborhood U_e of x, such that H induces on S/Se a finite group H_e. By the compactness of X, we cover X

with finitely many of these neighborhoods $\{U_e | e \in A\}$. Then H is embedded in the finite product of the finite groups H_e, $e \in A$, because if h in H induces the identity on every S/Se then h_x is the identity on every $S_x = S/Sx$ (since every x contains some e in A); from (2. 7) $h \to 1$ under $\mathrm{Hom}_R(S, S) \to \mathrm{Hom}_R(S, S)_x$; (2. 9) then implies $h = 1$. Thus H is finite.

(2. 17) *If S is an R-algebra and F is a finite group of R-algebra automorphisms of S, then for every x in X, $(S^F)_x = (S_x)^{F_x}$ where S^F denotes the fixed ring under F* (3. 3).

Proof. The inclusion $\subset$ is trivial. If $u \in S_x$ and $f_x(u) = u$ for every f in F, lift u to an element v in S and have $(f(v) - v)_x = 0$ for all (finitely many) f in F. By (2. 8), $f(v)(1 - e) = v(1 - e)$ for some e in x. If $s = v(1 - e)$, we have $s \in S^F$ and $s_x = v_x = u$, which completes the proof.

3. Galois theory.

Henceforth we consider a ring extension $R \subset S$ satisfying the following hypotheses.

(3. 1) Definition. A commutative R-algebra S is said to be *weakly Galois* (over R) provided

(3. 1a) S is a finitely generated, faithful, projective R-module, and a separable R-algebra.

(3. 1b) The S-module $\mathrm{Hom}_R(S, S)$ is generated by R-algebra automorphisms of S. If $\rho: S \to \mathrm{Hom}_R(S, S)$ is the usual *regular representation* of S, $\rho(s)(t) = st$, then (3. 1b) may be phrased thus:

(3. 1c) $\rho(S)G = \mathrm{Hom}_R(S, S)$.

See also (3. 6) and (3. 15) for equivalent conditions.

(3. 2) *If S is weakly Galois over R, then for every x in X, S_x is weakly Galois over R_x.*

Proof. (3. 1a, b) are inherited under localizations.

(3. 3) Definition. If S is a ring and H is a set of automorphisms of S, we use S^H to denote the fixed ring $\{s \in S | h(s) = s$ for every h in $H\}$. If T is a subring of S, $\mathrm{Aut}_T(S)$ will denote the group of all automorphisms of S that are the identity on T.

(3. 4) *If S is weakly Galois over R and $G = \mathrm{Aut}_R(S)$, then $S^G = R$.*

If $s \in S^G$, then $\rho(s)$ commutes with G in $\mathrm{Hom}_R(S, S)$. Since S is commutative, $\rho(s)$ commutes with $\rho(S)$. Hence, by (3. 1c), $\rho(s)$ is in the center of $\mathrm{Hom}_R(S, S)$, which, because of (3. 1a) is $\rho(R)$. Hence $s \in R$.

In Section 4 we give an example to show that the converse of (3. 4) fails, even in the presence of (3. 1a). However, (3. 6), which gives an equivalent formulation of "weakly Galois", may be considered a kind of converse. The converse holds in the following form in the absence of idempotents:

(3. 5) *Suppose R has no idempotents but* 0 *and* 1. *If S satisfies* (3. 1a) *and if $S^H = R$ for some subgroup H of G, then $\rho(S)H = \mathrm{Hom}_R(S, S)$; in particular, the Galois theory in* [VZ] *applies if and only if S is weakly Galois over R.*

Proof. If $e_1, \cdots, e_n$ is the set of minimal idempotents in S, then H must be transitive on this set and Se_j must be H_j-Galois over R [VZ, 1. 3] where H_j is the subgroup of H that sends Se_j into itself. If ρ_j is the regular representation of Se_j, then this implies $\mathrm{Hom}_R(Se_j, Se_j) = \rho_j(Se_j)H_j$. If h_{ij} is an element of H sending e_i to e_j, then $\mathrm{Hom}_R(S, S) = \oplus_{i,j}\mathrm{Hom}_R(Se_i, Se_j) = \oplus_{i,j}\mathrm{Hom}_R(Se_j, Se_j)h_{ij} = \oplus_{i,j}\rho_j(Se_j)H_jh_{ij} \subset \rho(S)H$.

(3. 6) THEOREM. *Let S be an R-algebra satisfying* (3. 1a). *Then S is weakly Galois over R if and only if there is a finite group* (*equivalently, a finite set*) *of automorphisms of S having fixed ring R.*

Proof. Assume S is weakly Galois. By (3. 2) and (3. 5), the Galois theory in [VZ] applies to S_x for each x in X. That is, $\mathrm{Aut}_{R_x}(S_x)$ is a finite group with fixed ring R_x. Use (2. 14) to extend this finite group to automorphisms $h_1, \cdots, h_n$ of S. These will generate a finite group H, by (2. 16). By (3. 5), $(\rho(S)H)_x = \rho_x(S_x)H_x = \mathrm{Hom}_{R_x}(S_x, S_x) = \mathrm{Hom}_R(S, S)_x$ (of course, ρ_x is the regular representation of S_x). It follows by (2. 11) that $\rho_y(S_y)H_y = (\rho(S)H)_y = \mathrm{Hom}_R(S, S)_y$ for all y in a neighborhood of x. In particular, $(S_y)^{H_y} = R_y$ by (3. 4). For each x we have a finite group H and a neighborhood of x such that at each point y in the neighborhood, $(S_y)^{H_y} = R_y$. By compactness, we get a finite number of these neighborhoods covering X and a finite number of H's which then generate a finite group F with $(S_x)^{F_x} = R_x$ at every point x. By (2. 17) and (2. 11), $S^F = R$.

https://doi.org/10.1017/S0027763000013039 Published online by Cambridge University Press

Conversely, if F is finite and $S^F=R$, then for every x, $R_x=(S^F)_x=S_x{}^{F_x}$, which by (3. 5) and (2. 7) implies $\rho_x(S_x)F_x = \mathrm{Hom}_{R_x}(S_x, S_x) = \mathrm{Hom}_R(S,S)_x$. It then follows from (2. 11) that $\rho(S)F = \mathrm{Hom}_R(S,S)$, proving S is weakly Galois.

(3. 7)[2] DEFINITION. If H is a group of automorphisms of S, the *closure* of H is the set of all automorphisms g that satisfy either of the following equivalent conditions:

(3. 7a) For each x in X and each minimal idempotent f in S_x, $\rho_x(f)g_x = \rho_x(f)h_x$ for some h in H.

(3. 7b) For some set $\{E_i\}$ of idempotents in S with $\cup E_i=1$, $\rho(E_i)g=\rho(E_i)h_i$ for some h_i in H (all i).

H is *closed* if it equals its own closure.

The condition $\cup E_i = 1$ in (3. 7b), of course, is a statement in the Boolean algebra $B(S)$; it means that if E is an idempotent in S and $EE_i = E_i$ for all i, then $E = 1$. However, for comparison between (3. 7a) and (3. 7b), another condition is more convenient: for every x in X and for every minimal idempotent f in S_x there is some i such that $E_{ix} \geq f$, that is $E_{ix}f = f$. The proof that these two conditions are equivalent is not difficult and runs along our typical line of extension arguments.

We now prove the equivalence of (3. 7a) and (3. 7b). If g satisfies (3. 7a), lift each f in each S_x to an idempotent E_f in S by (2. 12), and consider the two elements $u = \rho(E_f)g$ and $v = \rho(E_f)h$ in $\mathrm{Hom}_R(S,S)$, where h is the element of H given in (3. 7a) such that $\rho_x(f)g_x = \rho_x(f)h_x$. By (2. 7) we conclude the images of u and v in $\mathrm{Hom}_R(S,S)_x$ are equal.

By (2. 9), $u(1-e) = v(1-e)$ for some $e \in x$. Write $E'_f = (1-e)E_f$. Then $\rho(E'_f)g = \rho(E'_f)h$ and $(E'_f)_x = (1-e)_x(E_f)_x = f$.

Conversely, for each minimal idempotent f in S_x, choose an E_i such that $E_{ix}= f$. Then $\rho(E_i)g = \rho(E_i)h_i$ implies $\rho_x(E_{ix})g_x = \rho_x(E_{ix})h_{ix}$, as desired.

(3. 8) THEOREM. *Let S be a weakly Galois R-algebra. Then the usual Galois correspondence* (3. 3) *is one-to-one between the set of all separable subalgebras of S and the set of all subgroups H of the automorphism group of S that satisfy* (3. 8c) *below, or, equivalently, that satisfy* (3. 8a) *and* (3. 8b):

---

[2] Added August 12, 1968: A. Magid has improved (3.7b) to $\rho(E_i)g=\rho(E_i)h_i$ for some finite set of orthogonal idempotents E_i with $\sum E_i=1$ and some h_i in H.

(3. 8a) *For some finite subgroup F of H, $S^F = S^H$.*

(3. 8b) *H is closed in the sense of* (3. 7).

(3. 8c) *H is the closure of some finite set (equivalently, some finite group) of automorphisms of S.*

Proof. We need to show five things:

(3. 9a) If T is separable and $H = \mathrm{Aut}_T(S)$, then H satisfies (3. 8a) and (3. 8b).

(3. 9b) If H is a subgroup of the automorphism group of S and H satisfies (3. 8a) and (3. 8b), then S^H is separable over R.

(3. 9c) If T is separable and $H = \mathrm{Aut}_T(S)$, then $T = S^H$.

(3. 9d) If H satisfies (3. 8a) and (3. 8b) and $T = S^H$, then $\mathrm{Aut}_T(S) = H$.

(3. 9e) (3. 8c) is equivalent to (3. 8a) and (3. 8b).

We begin with a stronger version of (3. 9b).

(3. 10) *If F is a finite subgroup of G, then S^F is a separable subalgebra of S.*

Proof. First, we argue that if $T = S^F$, then T is flat over R: For every x in X, $T_x = S_x^{F_x}$ by (2. 17), but this is separable over R_x by [VZ, Theorem p. 731]. Hence T_x is also projective and therefore flat over R_x. For every R-module A and every x, $(\mathrm{Tor}^R(T, A))_x = \mathrm{Tor}^{R_x}(T_x, A_x) = 0$. This implies $\mathrm{Tor}^R(T, A) = 0$ by (2. 11).

Since T and S are both flat over R, the mapping $T \otimes T \to S \otimes S$ is a monomorphism, and we may identify $T \otimes T$ with its image in $S \otimes S$. To prove T is separable, then, it suffices to produce an element f in $S \otimes S$ with the following properties

(3. 11a) $$f \in T \otimes T$$

(3. 11b) $$(1 \otimes t - t \otimes 1) f = 0 \text{ for all } t \text{ in } T$$

(3. 11c) $$\mu(f) = 1$$

where μ: $S \otimes S \to S$ is the multiplication map, for then $T \otimes T \to T$ will split as $(T \otimes T)$-module map, since a reverse map may be defined by the condition that it send 1 to f. This splitting implies T is separable.

Since S is separable μ splits, and the image of 1 under this reverse map is an element e in $S \otimes S$ having the properties $(1 \otimes s - s \otimes 1) e = 0$ for

all s in S and $\mu(e) = 1$. This e is unique due to the commutativity of S; since for every g in G, $(g \otimes g)(e)$ has these properties, we have $(g \otimes g)(e) = e$.

Now, for each h in F, write $e_h = (h \otimes 1)(e)$. Since $h \otimes 1$ is an $(R \otimes S)$-algebra automorphism of $S \otimes S$, $(1 \otimes s - h(s) \otimes 1) e_h = 0$ for all s in S. In particular, $(1 \otimes t - t \otimes 1) e_h = 0$ for all t in T.

Let f denote the union of the e_h,

$$f = 1 - \Pi_{h \in F}(1 - e_h).$$

Then (3. 11b) holds since it holds for each e_h, and (3. 11c) holds because $\mu(1 - e) = 0$ and so $\mu(\Pi (1 - e_h)) = 0$. It remains to show that $f \in T \otimes T$. It is clear that $f \in (S \otimes S)^{F \otimes F}$ because for all h, h', h'' in F,

$$(h' \otimes h'')(e_h) = (h'h \otimes h'')(e) =$$
$$= (h'hh''^{-1} \otimes 1)(h'' \otimes h'')(e) = (h'hh''^{-1} \otimes 1)(e) = e_{h' hh''^{-1}}$$

so $h' \otimes h''$ permutes the e_h's, and will leave f fixed. Therefore, it remains to show $(S \otimes S)^{F \otimes F} = T \otimes T$. If $h \in F$ then $S^{\{h\}} = \mathrm{Ker}\,(1 - h\colon S \to S)$, so, since S is flat over R, $S \otimes S^{\{h\}} = \mathrm{Ker}\,(1 - 1 \otimes h) = (S \otimes S)^{\{1 \otimes h\}}$. Further, if $S_1, \cdots, S_n$ are R-submodules of S, then $S \otimes (\cap_{i=1}^{n} S_i) = \cap (S \otimes S_i)$ (since $\cap S_i = \mathrm{Ker}(S \to \Pi (S/S_i))$ and tensoring with a flat module S preserves kernels and finite products of R-modules). Hence $S \otimes S^F = (S \otimes S)^{1 \otimes F}$. In the same way, since T is flat over R, $(S \otimes T)^{F \otimes 1} = S^F \otimes T$. Combining, $(S \otimes S)^{F \otimes F} = ((S \otimes S)^{1 \otimes F})^{F \otimes 1} = (S \otimes T)^{F \otimes 1} = T \otimes T$.

In view of (3. 4), the following is enough to prove (3. 9c):

(3. 12) *If S is weakly Galois over R and if T is a separable subalgebra of S then S is weakly Galois over T.*

Proof. If T is separable, then T is finitely generated as an R-module [AB, 4. 7 and 4. 8], say by a finite set N. Use (2. 14) to conclude that $H = \mathrm{Aut}_T(S)$ induces on S_x the full automorphism group of S_x over T_x, for each x in X. Then by (3. 5) and (2. 7) $\rho_x(S_x)H_x = \mathrm{Hom}_{T_x}(S_x, S_x) = \mathrm{Hom}_T(S, S)_x$ (this last equality needs the fact that S is finitely generated and projective over T, which also comes from [AB, 4. 8]). It then follows from (2. 11) that $\rho(S)H = \mathrm{Hom}_T(S, S)$.

We have proved part of (3. 9a), namely (3. 8a), because (3. 12) asserts that S is weakly Galois over T and (3. 6) then implies that $S^F = T$ for some finite subgroup F of H. Combined with (3. 9c), this gives (3. 8a).

To complete the proof of (3. 9a), it suffices to show

(3. 13) *For every subalgebra T of S, $\mathrm{Aut}_T(S)$ is closed.*

Proof. If g is an automorphism such that, for every x in X and every minimal idempotent f in S_x, $\rho_x(f)g_x = \rho_x(f)\, h_x$ for some h in $\mathrm{Aut}_T(S)$, then for every t in T, $fg_x(t_x) = \rho_x(f)g_x(t_x) = \rho_x(f)h_x(t_x) = ft_x$. Since the sum of all f in S_x is 1, we have $g_x(t_x) = t_x$ or $g(t)_x = t_x$ for every x. By (2. 9), $g(t) = t$ and so $g \in \mathrm{Aut}_T(S)$.

(3. 14) *If F is a finite group of automorphisms of S and if $T = S^F$, then $\mathrm{Aut}_T(S)$ is contained in the closure of F.*

Proof. Suppose $g \in \mathrm{Aut}_T(S)$. Then for every x in X g_x is an automorphism of S_x that is the identity on T_x, and $T_x = S_x^{F_x}$, according to (2. 17). By [VZ, Theorem] g_x is in the "fat group generated by F_x", that is, for every minimal idempotent f in S_x, $\rho_x(f)g_x = \rho_x(f)h_x$ for some h_x in F_x. This is the same as saying g is in the closure of F.

This completes the proof of (3. 14). (3. 9d) follows immediately: If H is any group satisfying (3. 8a) and (3. 8b) and if $T = S^H = S^F$ with F a finite subgroup of H, then since the closure operation preserves inclusions, the closure of F is contained in H. But $T = S^H$ implies that $H \subset \mathrm{Aut}_T(S)$, and we have just proved in (3. 14) that $\mathrm{Aut}_T(S)$ is contained in the closure of F. Hence $H = \mathrm{Aut}_T(S) =$ closure of F. Notice that we have simultaneously proved (3. 9d) and half of (3. 9e): (3. 8a) and (3. 8b) imply (3. 8c).

To complete the proof of (3. 9e), suppose H satisfies (3. 8c), write $H =$ the closure of F with F finite, and set $T = S^F$. According to (3. 14), $\mathrm{Aut}_T(S) \subset H$. By (3. 13) and because $F \subset \mathrm{Aut}_T(S)$, $H \subset \mathrm{Aut}_T(S)$, which means $H = \mathrm{Aut}_T(S)$. Since T is separable by (3. 10), we may use (3. 9c) to conclude that $T = S^H$, so that H satisfies (3. 8a). It is a triviality that every closure is closed, so H satisfies (3. 8b).

We can now compare our weakly Galois hypothesis with that of Kreimer. His condition is this:

(3. 15) *There exists a finite set of orthogonal idempotents $\{e_1, \cdots, e_n\}$ in R with $\sum e_i = 1$ and with Se_i Galois over Re_i for each i.*

This clearly implies weakly Galois, but we shall also prove the converse. First, if S is weakly Galois over R we show that S_* is Galois over R_*

https://doi.org/10.1017/S0027763000013039 Published online by Cambridge University Press

for each x in X. If $S_x = \Pi S_i$ is a decomposition of S_x into indecomposable R_x-algebras, then all the S_i must be isomorphic, else the sum of the identity elements of those S_i that are in one isomorphism class will be a proper idempotent in S_x that is invariant under all automorphisms, hence will be a proper idempotent in R_x, contradicting (2. 13). Now choose one isomorphism α_i: $S_1 \to S_i$ for each i and construct an automorphism α of S_x by demanding that α restricted to S_i be $\alpha_{i+1} \circ \alpha_i^{-1}$ for $i < n$ and α restricted to S_n be α_n^{-1}. Let H be the cyclic group generated by α and let G_x be the product of H and the automorphism group of S_1 over R_x. Then S_x will be G_x-Galois over R_x (the elements of G_x are strongly distinct in the sense of [CHR, 1. 1]).

Now lift G_x to a set of automorphisms of S by (2. 14). The multiplication table that holds at x will hold in a neighborhood U_e of x, so this lifted set will be a group in U_e, isomorphic to G_x. If $Se[G]$ denotes the usual crossed product (with trivial factor set) of G over the ring Se, we have the homomorphism θ: $Se[G] \to \mathrm{Hom}_{Re}(Se, Se)$. We know this induces an isomorphism at x, since the definition of "S_x is G_x-Galois over R_x" requires $S_x[G_x] \to \mathrm{Hom}_{R_x}(S_x, S_x)$ be an isomorphism and the localization at x of $Se[G]$ is $S_x[G_x]$ and of $\mathrm{Hom}_{Re}(Se, Se)$ is $\mathrm{Hom}_{R_x}(S_x, S_x)$. If C denotes the cokernel of θ, then $C_x = 0$; but C is finitely generated over Re since $\mathrm{Hom}_{Re}(Se, Se)$ is, so C is zero in some neighborhood of x, that is $Ce' = 0$ for some e' with $x \in U_{e'} \subset U_e$. Hence θ': $Se'[G] \to \mathrm{Hom}_{Re'}(Se', Se')$ is an epimorphism. But $\mathrm{Hom}_{Re'}(Se', Se')$ is projective over Re', so the kernel of θ' is a direct summand in $Se'[G]$, hence finitely generated over Re'. The same localization argument then shows that this kernel is also zero in some smaller neighborhood of x. Thus for every x in X there is a neighborhood $U_{e''}$ of x such that $Se''[G] \to \mathrm{Hom}_{Re''}(Se'', Se'')$ is an isomorphism, that is Se'' is G-Galois over Re''. A finite number of neighborhoods cover X. Using the usual Boolean operations and noticing that if Se is G-Galois over Re, then Se' is G-Galois over Re' for every e' with $U_{e'} \subset U_e$, we can arrange that these neighborhoods $U_{e_1}, \cdots, U_{e_n}$ are disjoint. Then $\{e_1, \cdots, e_n\}$ is the required set of idempotents.

4. Two examples.

First we show that in the Galois correspondence, we must restrict ourselves to groups satisfying (3. 8a) and (3. 8b); the latter closure condition is not enough by itself.

Let X be $\{1, 1/2, 1/3, \cdots, 1/n, \cdots, 0\}$ with its relative topology as a subset of the real line and let W be the ring of continuous functions from X to the discrete field Q of rational numbers. In other words, W is the result of adjoining an identity to a countable ring-direct sum of copies of Q. The Boolean spectrum of W is indeed X and $w_x = w(x)$ for each w in W. Let K be a Galois extension field of Q with Galois group G and let V be the ring of continuous functions from X to K. Then V is weakly Galois over W since $V = K \otimes_Q W$ and $V^{(G\otimes 1)} = W$ (in fact, the extension is even strongly Galois). Consider the subgroup H of $\mathrm{Aut}_W(V)$ consisting of all automorphisms g such that g is the identity at the point 0 in X. Then H is closed, $H \neq \mathrm{Aut}_W(V)$, but $V^H = W$ because if $v \notin W$ then $v_x \in Q$ for some x and hence for some $x \neq 0$; and H contains an automorphism h such that $h_y =$ identity for all $y \neq x$ and $h_x(v_x) \neq v_x$ so that $h(v) \neq v$. This shows that H and $\mathrm{Aut}_W(V)$ cannot both fit into a Galois correspondence.

The second example shows that without assuming S is weakly Galois, the partial assumptions (3. 1a) and $S^G = R$ for some G are not sufficient to carry out our Galois theory.

Let W be as above, let e_n denote the idempotent characteristic function of the one-point set $\{1/n\}$ and let R be $W[t, u]/I$ with t and u indeterminates over W and I the ideal generated by $tu - 1$ and all $te_n + n^4 e_n$ for $n = 1, 2, \cdots$. Let α denote the residue class of t in R. The Boolean spectrum of R is still X, $R_x = Q$ for all $x \neq 0$ and $R_0 = Q[t, t^{-1}]$ with $t = \alpha_x$ indeterminate over Q. Let S be the result of adjoining a fourth root β of α to R, so $S = R[v]/(v^4 - \alpha)$. Then S has a free basis $1, \beta, \beta^2, \beta^3$ over R and is separable because $e = (1/4)(1 \otimes 1 + \beta \otimes \beta^{-1} + \beta^2 \otimes \beta^{-2} + \beta^3 \otimes \beta^{-3})$ is an element of $S \otimes_R S$ satisfying $\mu(e) = 1$ and $e(\beta \otimes 1 - 1 \otimes \beta) = 0$ so $e(x \otimes 1 - 1 \otimes x) = 0$ for all x in S. We now show $S^G = R$. If $x \neq 0$ then $S_x = Q[\sqrt[4]{-n^4}] = Q[\sqrt[4]{-1}]$, a Galois extension field of $R_x = Q$. Thus any element s of S that is invariant under all automorphisms of S will have $s_x \in R_x$ for all $x \neq 0$. To show that in fact $s \in R$, write $s = a + b\beta + c\beta^2 + d\beta^3$ with $a, b, c, d \in R$. Since $s_x = a_x + b_x\beta_x + c_x\beta_x^2 + d_x\beta_x^3 \in R_x$, we must have $b_x = c_x = d_x = 0$ for all $x \neq 0$. By (2. 9), if we show $b_0 = c_0 = d_0 = 0$ then $b = c = d = 0$ and $s \in R$. Now $b = \sum_{i=m}^{n} a_i \alpha^i$ with $a_i \in W$ and $b_x = \sum a_i(x) \alpha_x{}^i = 0$ for all $x \neq 0$. Since $a_0, \cdots, a_n$ are continuous functions, all $a_i(x)$ are constant $(= a_i(0))$ on some neighborhood of 0. Thus we have a single polynomial $\sum a_i(0) t^i$ in $Q[t, t^{-1}]$ with infinitely many roots, namely $\alpha_x = -n^4$ for all integers n.

This polynomial must be 0, so $a_i(0) = 0$ for all i. Thus $b_0 = 0$. Similarly, $c_0 = d_0 = 0$ and we have proved $S^G = R$.

On the other hand, we show that $S_0^{G_0} \neq R_0$ which, by (2. 17) and (3. 6), show that S is not weakly Galois over R and also shows that our technique of reducing to the case of no idempotents will not work here. As we said, $R_0 = Q[t, t^{-1}]$ with t indeterminate over Q; and $S_0 = R_0[\beta_0]$ with $\beta_0^4 = t$.

Then S_0 is contained in the rational function field $Q(\beta_0)$ (β_0 is indeterminate over Q) and contains no fourth roots of 1 except ± 1. If g is an R_0-algebra automorphism of S_0, it carries β_0 to another fourth root of t, which must be β_0 times a fourth root of 1. Hence $g(\beta_0) = \pm\beta_0$ and $g(\beta_0^2) = \beta_0^2$. Thus β_0^2 is in $S_0^{G_0}$ but not in R_0.

References

[AB] M. Auslander and D.A. Buchsbaum, *On ramification theory in Noetherian rings*, Amer. J. Math. **81** (1959) 749–765.

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

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

[CHR] S.U. Chase, D.K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Memoirs Amer. Math. Soc. No. 52, 1965.

[K] H.F. Kreimer, *A note on the outer Galois theory of rings*, to appear in Pacific J. Math.

[P] R.S. Pierce, *Modules over commutative regular rings*, Memoirs Amer. Math. Soc. No. 70, 1967.

[VZ] O.E. Villamayor and D. Zelinsky, *Galois theory for rings with finitely many idempotents*, Nagoya Math. J. **27** (1966) 721–731.

Northwestern University