Can. J. Math., Vol. XXIV, No. 4, 1972, pp. 573–579

GALOIS THEORY OF ESSENTIAL EXTENSIONS OF MODULES

SYLVIA WIEGAND

The purpose of this paper is to exploit an analogy between algebraic extensions of fields and essential extensions of modules, in which the role of the algebraic closure of a field F is played by the injective hull $H(M)$ of a unitary left R-module M. (The notion of "algebraic" extensions of general algebraic systems has been studied by Shoda; see, for example [5].)

In this analogy, the role of a polynomial $p(x)$ is played by a homomorphism of R-modules

$$f : I \to M \quad (I \text{ a left ideal of } R) \tag{1}$$

which will be called an *ideal homomorphism* into M. The process of solving the equation $p(x) = 0$ in F, or in an algebraic extension of F, will be replaced by the process of extending an ideal homomorphism (1) to a homomorphism f^* from R into M, or into an essential extension of M. Since such an extension f^* of f is completely determined by $f^*(1)$, any element of the form $x = f^*(1)$ in an essential extension E of M will be called a *root of* f (in E).

The key to the analogy between algebraic closure and injectivity is given by "Baer's criterion for injectivity" which states, in the terminology above: Given ${}_RM$, if every ideal homomorphism into M has a root in M, then M is injective.

To continue the analogy, we define the *splitting module*, over M, of a set of ideal homomorphisms $f_j : I_j \to M$ to be the submodule S of $H(M)$ generated by M and all the roots in $H(M)$ of the given homomorphisms; that is

$$S = M + \sum Rx \quad (x = f_j^*(1))$$

where the summation extends over all possible extensions f_j^* of f_j.

Finally, given a module ${}_RS \supseteq M$, we define $\mathcal{G}(S|M)$, the *Galois group of* S *over* M, to be the set of all automorphisms of ${}_RS$ that induce the identity on M.

The first section demonstrates that the injective hull and splitting module have the same closure properties as the algebraic closure and splitting field. For example, it is shown that if $M \subseteq {}_RS \subseteq H(M)$, then S is a splitting module for some family of ideal homomorphisms into M if and only if S is stable under the Galois group of $H(M)$ over M.

Received June 17, 1971 and in revised form, December 22, 1971. The author is indebted to Lawrence Levy for suggesting the problem, as well as for his advice and encouragement. This paper will form part of the author's Ph.D. thesis. This research was partially supported by an NSF Graduate Fellowship.

As in the case of field theory, the deeper results require a finiteness hypothesis. The main result of § 2 states that if ${}_R(R/I)$ has DCC, then the Galois group of the splitting module of any family of homomorphisms from I to M is solvable.

In the third section we show that if R is noetherian, then Baer's criterion can be improved to state: If ${}_RE$ is an essential extension of ${}_RM$ and every ideal homomorphism from I to M has a root in E, then E is the injective hull of M. We show by an example that the hypothesis "noetherian" cannot be dropped.

1. Basic properties of essential extensions. In this section, assume M is a left R-module imbedded in $H(M)$, an injective hull of M.

LEMMA 1.1. *If x and y are roots of an ideal homomorphism $f: I \to M$, then $I(x - y) = 0$.*

Proof. Put $x = f^*(1)$, $y = f'(1)$, where both f^* and f' extend f, and let $r \in I$. Then

$$r(x - y) = rf^*(1) - rf(1) = f(r) - f(r) = 0.$$

Definitions. An ideal homomorphism $f: I \to M$ is *irreducible* if f cannot be extended to any homomorphism $f^*: K \to M$, with K a strictly larger left ideal. For $x \in H(M)$, let $I = \{r \in R: rx \in M\}$. Then I is a nonzero left ideal of R, because $H(M)$ is an essential extension of M. The ideal homomorphism $f: I \to M$, given by $f(i) = ix$ for each $i \in I$, will be called the *irreducible homomorphism of x over M* (the analogue of the minimum polynomial of an element of an algebraic field extension).

To justify the terminology, we show that every other ideal homomorphism $h: J \to M$ with x as a root is extended by f (that is, $J \subseteq I$ and $h = f$ on J), and that f is irreducible. First, since $Jx = h(J) \subseteq M$, we must have $J \subseteq I = \{r \in R: rx \in M\}$, and for each $r \in J$, $h(r) = rx = f(r)$. To see that f is irreducible, suppose $g: K \to M$ is a proper extension of f. Let $k \in K - I$, so that $kx \notin M$. Now, there exists an r in R with $0 \neq r(g(k) - kx) \in M$, since $H(M)$ is an essential extension of M. Since $rg(k) \in M$, it follows that $rkx \in M$, so $rk \in I$. Hence $r(g(k) - kx) = g(rk) - f(rk) = 0$, which is a contradiction.

PROPOSITION 1.2. *Let x and y be elements of $H(M)$. Then x and y are conjugate over M (that is, there exists a $\sigma \in \mathcal{G}(H(M)|M)$ with $\sigma(x) = y$) if and only if x and y have the same irreducible ideal homomorphism over M.*

Proof. The "only if" implication is trivial. For the other implication, let the common irreducible ideal homomorphism be $f: I \to M$. Note that $M + Rx \cong M + Ry$ by $\rho(m + rx) = m + ry$.

ρ is well-defined, because if $m + rx = 0$, then $r \in I = \{r \in R: rx \in M\}$. Thus $r(x - y) \in I(x - y) = 0$ by Lemma 1.1. So $rx = ry$ and $0 = m + rx = m + ry = \rho(m + rx)$. The same argument, read backwards, shows ρ is one-to-one.

Since $H(M)$ is injective, there is a homomorphism $\sigma: H(M) \to H(M)$ extending $\rho; \sigma$ is one-to-one because, otherwise, $(\ker \sigma) \cap M \neq 0$. Hence $\sigma(H(M))$ is an injective module. Since $M \subseteq \sigma(H(M)) \subseteq H(M)$ and $H(M)$ is the injective hull of M, σ must be onto. Now $\sigma \in \mathcal{G}(H(M)|M)$ as desired.

PROPOSITION 1.3. *For ${}_RS$ with $M \subseteq S \subseteq H(M)$, these are equivalent:*

(i) *S is the splitting module for some set of ideal homomorphisms into M.*

(ii) *If $S \subseteq {}_RE \subseteq H(M)$, then $\tau(S) = S$ for each $\tau \in \mathcal{G}(E|M)$.*

(iii) *If $f: I \to M$ is an irreducible ideal homomorphism and f has at least one root in S, then all roots of f are in S. (That is, every element of $H(M)$ that is a root of f lies in S.)*

Proof. (i) $\Rightarrow$ (ii) Assume S is the splitting module of $\{f_j: I_j \to M\}$, and let x be a root of f_j. By (1.2), $\tau(x)$ is also a root of f_j (and is therefore in S). Thus $\tau(S) \subseteq S$, and, applying the same argument to τ^{-1}, we get $\tau^{-1}(S) \subseteq S$; that is, $S = \tau(S)$.

(ii) $\Rightarrow$ (iii) Let x, y be roots of f, where $x \in S$. Then (1.2) shows there is a σ in $\mathcal{G}(H(M)|M)$ with $\sigma(x) = y$, and thus, by (ii), $y \in S$.

(iii) $\Rightarrow$ (i) For $s \in S$, let f_s be the irreducible ideal homomorphism of s over M. By (iii), S is the splitting module of $\{f_s: s \in S\}$ over M.

2. Solvability and finiteness. Again, ${}_RM$ and all splitting modules over M are to be considered inside a fixed injective hull $H(M)$ of M.

LEMMA 2.1. *Let ${}_RS$ be an essential extension of M and let A be a subset of S. Suppose that I is a left ideal of R such that $IA = 0$, and that $K \supset I$ is a left ideal with ${}_R(K/I)$ simple. Then $KA \subseteq M$.*

Proof. Let $a \in A$. If $Ka = 0$, then $Ka \subseteq M$. If $Ka \neq 0$, then since multiplication by a is a nonzero homomorphism from K into Ka, we deduce that Ka is simple. Now S essential over M implies $Ka \subseteq M$.

INDUCTION LEMMA 2.2. *Let $S \supseteq N \supseteq M$, where S and N are splitting modules over M. Then $\mathcal{G}(S|N) \lhd \mathcal{G}(S|M)$ and $\mathcal{G}(S|M)/\mathcal{G}(S|N) \cong \mathcal{G}(N|M)$.*

Proof. By (1.3) (stability of splitting modules) there is a "restriction homomorphism" $\Phi: \mathcal{G}(S|M) \to \mathcal{G}(N|M)$. Then $\ker(\Phi) = \mathcal{G}(S|N)$, so $\mathcal{G}(S|N) \lhd \mathcal{G}(S|M)$. To see that Φ is onto, take any $\rho \in \mathcal{G}(N|M)$ and extend it to σ in $\mathcal{G}(H(M)|M)$. By (1.3) again, σ induces $\tau \in \mathcal{G}(S|M)$, and $\Phi(\tau) = \rho$.

THEOREM 2.3. *Let S be a splitting module for a family $\mathcal{F}$ of ideal homomorphisms from a left ideal I into M. If ${}_R(R/I)$ has a composition series, then $\mathcal{G}(S|M)$ is a solvable group.*

Proof. We use induction on the composition length n of ${}_R(R/I)$. If $n = 0$, then $S = M$ and the Galois group is trivial. Assume $n > 0$, and choose a left ideal J such that ${}_R(J/I)$ is simple. By the induction lemma, it will suffice to

https://doi.org/10.4153/CJM-1972-051-x Published online by Cambridge University Press

find a splitting module N over M such that $\mathcal{G}(N|M)$ is abelian and S is the splitting module of some family of ideal homomorphisms from J to N.

Choose $k \in J$ such that $J = I + Rk$, and let W be the set of all roots of all $f \in \mathcal{F}$; set

$$N = M + \sum Rkx (x \in W).$$

Then (1.3) implies that N is a splitting module over M. Also S is the splitting module over N of all extensions of the family $\mathcal{F}$ to I (that is, we use multiplications by the x's on J).

For each $x \in W$, define the function φ_x: $\mathcal{G}(N|M) \to S$ by $\varphi_x(\sigma) = \sigma(kx) - kx$. Now x is a root of an ideal homomorphism f: $I \to M$, so by (1.2) if we consider σ as any extension to $\mathcal{G}(H(M)|M)$, $\sigma(x)$ is also a root of f. Thus $I(\sigma(x) - x) = 0$ (1.1), so $J(\sigma(x) - x) \subseteq M$ by (2.1). In particular, $\sigma(kx) - kx = k(\sigma(x) - x) \in M$; that is, the image of φ_x is in M.

We show φ_x is a group homomorphism φ_x: $\mathcal{G}(SM) \to (M, +)$:

$$\begin{aligned}\varphi_x(\sigma\tau) &= \sigma\tau(kx) - kx = \sigma\tau(kx) - \sigma(kx) + \sigma(kx) - kx \\ &= \sigma(\tau(kx) - kx) + \sigma(kx) - kx \\ &= \sigma(kx) - kx + \tau(kx) - kx,\end{aligned}$$

since $\varphi_x(\tau)$ is in M and M is an abelian group. Thus $\varphi_x(\sigma\tau) = \varphi_x(\sigma) + \varphi_x(\tau)$.

Now let φ: $\mathcal{G}(N|M) \to \Pi M^{(x)}$ ($M^{(x)}$ is a copy of M) be defined by $\varphi(\sigma) = (\varphi_x(\sigma))_x$. Then φ is a group homomorphism since φ_x is. Also φ is one-to-one, since if $\varphi_x(\sigma)$ is 0 for each x, then $\varphi(kx) = kx$ for each x. Therefore σ is the identity map on $N = M + \sum Rkx$.

We have shown $\mathcal{G}(N|M)$ may be imbedded, as a group, in an R-module. Thus $\mathcal{G}(N|M)$ is abelian.

Remark. By refining the inductive step in the above theorem slightly, we could have shown that if N', M' correspond to N and M at any stage of the induction, then $\mathcal{G}(N'|M')$ may be imbedded as a group in $\Pi M^{(x)}$. This gives us the following sharper version of Theorem 2.3:

If $S, \mathcal{F}$, I, M are as in (2.3), *then $\mathcal{G}(S|M)$ has a solvable series*

$$I = G_0 \lhd G_1 \lhd \ldots \lhd G_n = \mathcal{G}(S|M)$$

such that each G_i/G_{i-1} $(i = 1, \ldots, n)$ may be imbedded in a Cartesian power of M.

Proof. At the tth stage of the induction, replace (2) by

$$\sigma_t(x) - x \in \mathrm{Ann}_{H(M)} J_{t-1} \ (\sigma \in \mathcal{G}(N_t|N_{t-1})). \tag{3}$$

Now Lemma 2.1 shows that $k_t(\sigma(x) - x) \in M$, as desired.

Theorem 2.3 states conditions which imply that the Galois group is solvable; happily it is not always abelian under these conditions, as shown by the following example.

https://doi.org/10.4153/CJM-1972-051-x Published online by Cambridge University Press

Example. Let $\mathbf{Z}$ be the ring of integers, and set $I = 4\mathbf{Z}$, $M = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. Define $f: I \to M$ by $f(4) = (\bar{1}, \bar{0})$. Then f is irreducible. Let S be the splitting module of f over M. Then $x = (1 + (8\mathbf{Z}), 0)$ is a root of f in $\mathbf{Z}(2^\infty) \oplus \mathbf{Z}(2^\infty)$, the injective hull of M. Other roots of f are

$$y = x + (0, 1 + (4\mathbf{Z})) = (1 + (8\mathbf{Z}), 1 + (4\mathbf{Z}))$$

and

$$z = 3x = (3 + (8\mathbf{Z}), 0.$$

By transitivity of the Galois group (1.2), there exist σ, τ in $\mathcal{G}(S|M)$ with $\sigma(x) = y$ and $\tau(x) = z$. Then

$$\sigma\tau(x) = \sigma(3x) = 3\sigma(x) = 3y = 3x + (0, 3 + (4\mathbf{Z})).$$

On the other hand,

$$\tau\sigma(x) = \tau(y) = \tau(x) + \tau(0, 1 + (4\mathbf{Z})) = 3x + (0, 1 + (4\mathbf{Z})),$$

since $(0, 1 + (4\mathbf{Z})) \in M$. Therefore $\sigma\tau \neq \tau\sigma$ and $\mathcal{G}(S|M)$ is not abelian.

Unlike a polynomial, which can have only a finite number of roots, an ideal homomorphism almost always has an infinite number of roots: If x is a root of $f: I \to M$ in $H(M)$, then the set of all roots of f is easily seen to be $\{x + a: a \in \mathrm{Ann}_{H(M)}I\}$. In view of this, we can ask when the roots of f are "finitely generated," in the sense that the splitting module S of f is generated by M and a finite number of roots of f.

If M is finitely generated, the answer will be "yes" when R is a finite-dimensional algebra over a field, or when R is commutative with DCC, for then, by a result of Rosenberg and Zelinsky [**4**], $H(M)$ will be a finitely generated module.

The following theorem shows that S can be finitely generated over M even when $H(M)$ is not finitely generated; but strong finiteness and commutativity hypotheses seem to be required.

THEOREM 2.6. *Let S be a splitting module of an ideal homomorphism $f: I \to M$ and suppose*

(i) ${}_RM$ *is finitely generated,*

(ii) R *is an algebra over a commutative noetherian ring K and is finitely generated as a K-module, and*

(iii) ${}_R(R/I)$ *has a composition series.*

Then S can be generated by M and a finite number of roots of f.

Proof. Let $A = \mathrm{Ann}_{H(M)}I$, let x be one root of f, and let $\{x_i\}$ be all the roots of f in $H(M)$. Then, since $\{x_i\} = x + A$,

$$S = M + \sum Rx_i = M + Rx + RA.$$

(Note that A is a K-module but need not be an R-module.) It suffices to show that ${}_KA$ is finitely generated (and hence RA is a finitely generated R-module.)

https://doi.org/10.4153/CJM-1972-051-x Published online by Cambridge University Press

We prove this assertion by induction on the composition length t of ${}_R(R/I)$. If $t = 0$ the statement is trivial. Assume $t > 0$. Choose a left ideal J such that ${}_R(J/I)$ is simple, and write $J = I + Rj$. By Lemma 2.1, $(I + Rj)A \subseteq M$ and hence $jA \subseteq M$. Now, ${}_RM$ is finitely generated and so is ${}_KR$; hence ${}_KM$ is finitely generated. Since K is noetherian, the K-submodule jA of ${}_KM$ is finitely generated over K, say, by $ja_1, \ldots, ja_n$. That is, for each $a \in A$, we can choose $k_1, \ldots, k_n \in K$ such that $ja = k_1ja_1 + \ldots k_nja_n$. Since $k_i \in K$, $ja = j(k_1a_1 + \ldots + k_na_n)$, or $j(a - k_1a_1 - \ldots - k_na_n) = 0$. Therefore $a - k_1a_1 - \ldots - k_na_n \in \mathrm{Ann}_{H(M)}(I + Rj)$. It follows that

$$A \subseteq Ka_1 + \ldots + Ka_n + \mathrm{Ann}_{H(M)}(I + Rj) \subseteq A = \mathrm{Ann}_{H(M)}(I).$$

Now $\mathrm{Ann}_{H(M)}(I + Rj)$ is finitely generated over K by the inductive hypothesis, and so ${}_KA$ is finitely generated, as desired.

The result above is not true if condition (iii) is weakened to "${}_R(R/I)$ has ACC" even if R is commutative and f is irreducible. As an example, let $R = \mathbf{Z}[x]$, $I = (x)$, $M = R/I \cong \mathbf{Z}$, and define $f\colon (x) \to \mathbf{Z}$ by $f(x) = 1$. Note that ${}_R\mathbf{Q}$ with R-action $xq = 0$ is an essential extension of ${}_R\mathbf{Z}$, and so $\mathbf{Q} \subseteq \mathrm{Ann}_{H(M)}(x)$. But ${}_R\mathbf{Q}$ is not finitely generated over ${}_R\mathbf{Z}$; therefore the splitting module of f is not finitely generated over M.

3. An improved Baer's criterion. For an algebraic extension K of a field F to be the algebraic closure of F, it suffices that each polynomial with coefficients in F has a root in K. (See, for example, [**2**].) Here we show that the analogous statement for modules is false in general, but is true if R satisfies a weakened ascending chain condition.

THEOREM 3.1. *Let ${}_RM$ be an R-module with injective hull H. Suppose that E is a submodule of H satisfying*

(*) *every ideal homomorphism $f\colon {}_RI \to {}_RM$ has a root in E.*

If R has ACC *on left ideals that are the annihilators of elements of H, then $E = H$.*

Proof. Suppose $x \in H - E$, and let $f_0\colon J_0 \to M$ be the irreducible homomorphism of x over M, that is, $J_0 = \{j \in R\colon jx \in M\}$ and $f_0(j) = jx$ for $j \in J_0$. Since H is an essential extension of M, there is an element $j \in R$ such that $0 \neq jx \in M$. Therefore

$$\mathrm{Ann}_R x \underset{\neq}{\subset} J_0.$$

By hypothesis, the ideal homomorphism $f_0\colon J_0 \to M$ has at least one root x_1 in E. Since x and x_1 are both roots of f_0, we have, for $j \in J_0$, $jx = f_0(j) = jx_1$. Thus $J_0 \subseteq \mathrm{Ann}_R(x - x_1)$.

Now, since $x \notin E$ and $x_1 \in E$, we have that $x - x_1 \notin E$. Therefore we can give the same treatment to $x - x_1$ that was given to x. This yields an element x_2 in E with

$$\mathrm{Ann}(x - x_1) \underset{\neq}{\subset} \mathrm{Ann}(x - x_1 - x_2).$$

https://doi.org/10.4153/CJM-1972-051-x Published online by Cambridge University Press

Continuing this process produces an infinite increasing sequence of annihilators, contradicting the chain condition. We conclude that $H = E$.

Example. The ACC hypothesis cannot be dropped in Theorem 3.1. Let R be a valuation ring with maximal ideal J and quotient field Q, and let $M = R/J$. Notice that Q/J is an essential extension of R/J, and that R-submodules of Q/J are totally ordered.

A theorem of Gill [**1**] and Matlis [**3**] states that the submodules of $H(R/J)$ are totally ordered by inclusion if and only if R is almost maximal. Hence if R is any valuation ring that is *not* almost maximal, the essential extension Q/J of R/J will *not* be injective. On the other hand, every ideal homomorphism $f\colon I \to R/J$ has a root in Q/J.

To see this, assume $f \neq 0$. Since R/J is simple, f is onto, and hence $\ker(f)$ is a maximal submodule of I. Choose $k \in I - \ker(f)$ such that $I = Rk + \ker(f)$. Since R is a valuation ring and $Rk \not\subseteq \ker(f)$, we have $Rk = I$. The desired extension of f is now defined as follows: Let $f(k) = kh$ for some $h \in Q/J$, and define $f^*(r) = rh$.

References

1. D. Gill, *Almost maximal valuation rings*, J. London Math. Soc. *4* (1971), 140–146.
2. R. Gilmer, *A note on the algebraic closure of a field*, Amer. Math. Monthly *75* (1968), 1101–1102.
3. E. Matlis, *Injective modules over Prüfer rings*, Nagoya Math J. *15* (1959), 57–69.
4. A. Rosenberg and D. Zelinsky, *Finiteness of the injective hull*, Math. Z. *70* (1959), 372–380.
5. K. Shoda, *Zur theorie der algebraischen Erweiterungen*, Osaka Math. J. *4* (1952), 133–144.

The University of Wisconsin,
Madison, Wisconsin;
The University of Nebraska,
Lincoln, Nebraska