The Journal of National Chengchi University Vol. 29, 1974

Galois Theory of the Essential Extensions of an R-MODULE

Chiu-Wen Leu.

Introduction: Every ring R contains an identity element 1 and every right R-module M_R is unitery right R-module (simply, R-module). If N_R is a submodule of the R-module M_R, we use the symbol $N_R \subseteq' M_R$ to denote M_R is an essential extension of N_R.

The purpose of this paper is to exploit the analogy between algebraic extension of fields and essential extension of R-modules. In this analogy, the role of the algebraic closure of a field is played by the injective hull H(M) of the R-module M_R and that of a polynomial is played by an ideal R-homomorphism $f: I_R \longrightarrow M_R$, where I is a right ideal of R. The process of solving the equation $p(x)=o$ in the field F or in an algebraic extension of F will be replaced by the process of extending an ideal R-homomorphism to an R-homomorphism $f: R_R \longrightarrow M_R$ from R into M_R or into an essential extension of M_R.

Definiton 1. An ideal R-homomorphism $f: I_R \longrightarrow M_R$ where I is a right ideal of R is called irreducible iff f cannot be extended to an ideal R-homomorphism $f: K_R \longrightarrow M_R$ where K is a right ideal of R properly containing I.

R. Baer (1) proved that an R-module M_R is injective if and only if for every right ideal I of the ring R and for any element $f \in \mathrm{Hom}_R(I_R, M_R)$ there exists an irreducible ideal R-homomorphism $f^* \in \mathrm{Hom}_R(R_R, M_R)$ given by $f^*(r) = f^*(1)r$, $\forall r \in R$ such that the following diagram commutes; that is, $f^* o j = f$, where $j: I \longrightarrow R$ is the canonical injection.

$$\begin{array}{ccccc} O & \longrightarrow & I_R & \overset{j}{\longrightarrow} & R_R \\ & & f \downarrow & \swarrow f^* & \\ & & M_R & & \end{array} \qquad \text{(exact)}$$

It is easily seen that if M_R is an injective R-module, the R-homomorphism f^* is completely determined by the element $f^*(1)$ which is in M_R for if $f^*(1)=x$, then $f^*(r)=f^*(1)r=xr$, for all $r \in R$.

In general, if M_R is not injective, the element $f^*(1)$ need not be in M_R, but in some essential extension of M_R, for example, in the injective hull of the R-module M_R. Thus, we have the following definition.

Definition 2. Let $f \in Hom_R (I_R, M_R)$ be an ideal R-homomorphism and let $f^* \in Hom_R(R_R, M_R)$ be the extension of f. any element of the form $x=f^*(1)$ in some essential extension S_R of M_R is said to be a root of f in S_R.

In this terminology, we can restate the R. Baer's theorem as follows: an R-module M_R is injective if and only if every ideal R-homomorphism into M_R has a root in M_R.

Proposition 1. If x and y are roots of an ideal R-homomorphism $f \in Hom_R (I_R, M_R)$, where I is a right ideal of R, then $(x-y)\, I=O$.

Proof: Let

f^* and $\bar{f}$ be extensions of f such that $f^*(1)=x$ and $\bar{f}(1)=y$. Thus, for any element $a \in I$, we have $(x-y)\, a=x\, a-y\, a=f^*(1)\, a-\bar{f}(1)\, a=f^*(1a)-\bar{f}(1a)$ $=f(a)-f(a)=o$. Hence $(x-y)\, I=o$. Q. E. D.

For each $x \in H(M)$, the injective hull of M_R, then we construct a nonzero right ideal $I_x=\{r \in R \mid x\, r \in M_R\}$. This is the first result of the following proposition.

Proposition 2. (a) I_x is a nonzero right ideal of R.
(b). Let the function $f_x : I_x \longrightarrow M_R$ be defined by $f_x(i)=x\, i, \forall\, i \in I_x$, then f_x is irreducible.
(c). Let the function $g: I \longrightarrow M_R$ be any ideal R-homomorphism having x as a root. Then $I \subseteq I_x$ and $f_x \ I_I=g$.

Proof:
(a). We show first that I_x is a right ideal of R. To do this, for any m, $n \in I_x$, then $x\, m=o$ and $x\, n=o$. Thus

$x(m+n)=x\, m+x\, n=o+o=o$. This shows that $m+n \in I_x$. Moreover, for any $m \in I_x$ and $r \in R$, we have $x(m\, r)=(x\, m)\, r=o\, r=o$. Hence $m\, r \in I_x$. Therefore, I_x is a right ideal of R.

Next, we show that $I_x \neq o$. It is trivial in case $x=o$. So we may assume that $x \neq o$. Since H(M) is the injective hull of M_R, it is an essential extension of M_R. Hence, by Proposition 1.2.1. (see the author's master thesis), there

exists $o \neq r \in R$ such that $o \neq x\ r \in M_R$. This shows that $r \in I_X$. Hence $I_X \neq o$.
(b). Suppose that there exists an ideal R-homomorphism $h: K \longrightarrow M_R$ properly extending f_X, where K is a right ideal of R properly containing I_X; $I_X \subsetneqq K$. For any $y \in K - I_X$, $y \in K$ and $y \notin I_X$. Since $y \notin I_X$, $x\ y \notin M_R$. Thus $h(y) - x\ y \neq o$. Since H(M) is an essential extension of M_R, there exists $o \neq r \in R$ such that $o \neq (h(y) - xy)\ r \in M_R$. That is, $o \neq h(y)\ r - x\ y\ r \in M_R$. Since $h(y) \in M_R$, $h(y)\ r \in M_R$. Hence $h(y)\ r - (h(y)\ r - x\ y) \in M_R$; that is, $x\ y\ r \in M_R$. Hence $x\ y \in I_x$. But then $(h(y) - x\ y)\ r = h(y)\ r - x\ y\ r = h(y\ r) - f_x(y\ r) = f_x(y\ r) - f_x(y\ r) = o$, a contradiction. Hence f_x is irreducible.
(c)· Let g^* be an extension of g such that $g^*(1) = x$. Then $g^*(i) = g(i)$, $\forall i \in I$. Thus, $g^*(i) = g^*(1\ i) = g^*(1)\ i = x\ i = g(i)$. Hence $x\ i = g(i)$, $\forall i \in I$. So $x\ I = g(I) \subseteq M_R$. This implies that $I \subseteq I_x$. Furthermore, for each $i \in I$,
$g(i) = g^*(i) = x\ i = f_x(i)$. Hence $g^* = f_x$ extending g. Q. E. D.

The function f_x: $I_x \longrightarrow M_R$ defined by $f_x(i) = x\ i$, $\forall i \in I_x$ in Proposition 2 will be called the irreducible ideal R-homomorphism of x over M_R. This is the analog of the minimum polynomial of an element of an algebraic field extension.

Definition 3. (2) Let $x, y \in H(M)$. Then x and y are said to be conjugate over M_R if there exists an M-automorphism φ of H(M) ($\varphi: H(M) \longrightarrow H(M)$ is an automorphism with $\varphi(m) = m$, $\forall m \in M_R$) such that $\varphi(x) = y$.

Proposition 3. Let x and y be elements of H(M) which are roots of the same irreducible ideal R-homomorphism over M_R. Then the mapping Ψ: $M + xR \longrightarrow M + yR$ defined by $\Psi(m + x\ r) = m + yr$, for $m \in M_R$, $r \in R$ is an isomorphismof $M + xR$ onto $M + yR$.

Proof:

The mapping Ψ is well-defined, because if $m + x\ r = o$, then $x\ r = -m \in M_R$, and hence $r \in I_x$. Since x and y are roots of the same irreducible ideal R-homomorphism over M_R. By Proposition 1 we have $(x - y)\ I_x = o$. Since $(x - y)\ r \in (x - y)\ I_x$, $(x - y)\ r = o$ or $x\ r = y\ r$. Hence $o = m + x\ r = m + y\ r$. This shows that Ψ is well-defined.

Clearly, Ψ is onto. Finally, we show that Ψ is one-one. If

$\Psi(m + xr) = O$, then $m + yr = O$. Thus $yr = -m \in M_R$ and hence $r \in I_y$.

Since x and y are conjugate over M_R, $I_x = I_y$. Thus, by Proposition 1, we have $(x-y) I_x = O$. Hence $(x-y) r \in (x-y) I_x = O$, so $xr = yr$. Thus, $m + xr = m + yr = O$. This shows that Ψ is one-one. Hence Ψ is an isomorphism of $M+xR$ onto $M+yR$.

Proposition 4. Let x and y be elements of H(M). Then x and y are conjugate over M_R if and only if x and y are roots of the same irreducible ideal R-homomorphism over M_R.

Proof: Suppose that x and y are roots of the same irreducible ideal R-homomorphism over M_R. Then, by Proposition 3, the mapping φ: $M+xR \longrightarrow M+yR$ defined by

$\varphi(m+xr) = m+yr$ for all $m \in M_R$ and all $r \in R$ is an isomorphism of $M+xR$ onto $M+yR$. Since H (M) is injective, and $M+xR$ and $M+yR$ are essential extensions of M_R, we have, by Eckmann and Schopf's theorem(3), can be extended to an isomorphism Φ: $H(M) \longrightarrow H(M)$. Thus $\Phi(x) = y$ and $\Phi(m) = m$, $\forall m \in M_R$. Hence x and y are conjugate over M_R. The converse part of the proof is trivial since there exists an $\Phi \in Hom_R$ (H (M), H(M)) such that Φ (x) = y.

Definition 4. Let S_R be such that $M_R \subseteq' S_R \subseteq H(M)$. Then the set of all M-automorphisms of S_R is called the Galois group of S_R over M_R and is denoted by G (S/M).

Definition 5. A submodule S_R of H(M) is called the splitting R-module over M_R of a collection of ideal R-homomorphisms $f_i : I_i \longrightarrow M_R$ (each I_i is a right ideal of R,) if it is generated by M_R and all the roots in H (M) of the given ideal R-homomorphisms f_i.

If a R-module $S_R \subseteq H(M)$ is a splitting R-module over M_R of a collection $\{f_i\}$ of ideal R-homomorphisms of I_i into M_R, then it is obvious that $S_R = M + xR$ where $x = f^*_i(1)$and the summation extends over all possible extensions f^*_i of f_i.

Proposition 5. Let S_R be such that $M_R \subseteq' S_R \subseteq H(M)$. Then S_R is a splitting R-module over M_R of a collection of ideal R-homomorphisms into M_R if and only if every M-automorphism of H(M) maps S_R onto itself (that is, for each $\varphi \in G(H(M)/M)$, $\varphi(S) = S$) and thus induces an M-automorphism of S_R.

Proof: (i). Suppose that S_R is a splitting R-module over M_R of a collection of $\{f_i\}$ of ideal R-homomorphisms $f_i: I_i \longrightarrow M_R$. Let x_i be a root of f_i, by Proposition 4, for each $\varphi \in G(H(M)/M)$, $\varphi(x_i)$, being a conjugate of x_i, is a root of f_i and hence $\varphi(x_i) \in S_R$. Thus $\varphi(S) \subseteq S_R$. Using the same arguement apply to the inverse function $\varphi^{-1} \in G(H(M)/M)$, we have $\varphi^{-1}(S) \subseteq S_R$. Hence $\varphi(S) = S_R$. (ii). Suppose, conversely, that every $\varphi \in G(H(M)/M)$ induces an M-automorphism of S_R. We show first that if $f: I \longrightarrow M_R$ is an irreducible ideal R-homomorphism having a root in S_R, then all roots of f are also in S_R. To do this, let x and y be roots of f with $x \in S_R$. By Proposition 4, x and y are conjugate over M_R and hence there exists an M-automorphism $\Psi \in G(H(M)/M)$ such that $\Psi(x) = y$. Then Ψ induces an M-automorphism of S_R, so $\Psi(x) = y \in S_R$. Next, for each $x \in S_R$, let f_x be the irreducible ideal R-homomorphism of x over M_R. Then, by the above arguement, S_R is the splitting R-module over M_R of the collection

$\{f_x \mid x \in S_R\}$. Q. E. D.

Proposition 5 says that any splitting R-module over M_R is stable relative to M_R and H(M). (4).

Corollary 1. Let S_R be such that $M_R \subseteq' S_R \subseteq H(M)$. Then S_R is a splitting R-module over M_R of a collection of ideal R-homomorphisms into M_R if and only if $S_R \subseteq' E_R \subseteq H(M)$ implies $\varphi(S) = S_R$, for each $\varphi \in G(E/M)$.

Proof: Suppose that S_R is a splitting R-module over M_R of a collection of ideal R-homomorphisms into M_R. Let $\varphi \in G(E/M)$. Then, since $S_R \subseteq' E_R$, $M_R \subseteq' E_R$ and hence $H(E) = H(M)$. By Eckmann and Schopf's theorem, φ can be extended to an M-automorphism Ψ of H(M). Since S_R is a splitting R-module over M_R, by Proposition 5, $\Psi(S) = S_R$. Hence $\varphi(S) = S_R$.

The proof of the converse part of the theorem is just the same as part (ii) of Proposition 5.

Q. E. D.

Proposition 6. Let S_R and N_R be splitting R-modules of M_R such that $M_R \subseteq' N_R \subseteq' S_R \subseteq H(M)$. Then

(i). G(S/N) is a normal subgroup of G(S/M).

(ii). $G(S/M) / G(S/N) \cong G(N/M)$.

Proof: For $\sigma \in G(S/M)$, since N_R is a splitting R-module of M_R, by

Proposition 5, σ induces an M-automorphism $\sigma_N \in G(N/M)$. The mapping Φ: $G(S/M) \longrightarrow G(N/M)$ defined by $\Phi(\sigma)=\sigma_N$ for $\sigma \in G(S/M)$ is obviously an R-homomorphism. Then the kernel of Φ is clearly $G(S/N)$. Hence $G(S/N)$ is a normal subgroup of $G(S/M)$. To show that Φ is also onto. For any $\sigma_N \in G(N/M)$, since $M_R \subseteq' N_R$, σ_N can be extended to an M-automorphism

$\varphi \in G(H(M)/M)$. By Proposition 5, since S_R is a splitting R-module over M_R, φ induces an M-automorphism $\sigma \in G(S/M)$ and $\Phi(\sigma)=\sigma_N$. Hence Φ is onto. Thus

$G(S/M)/G(S/N) \cong G(N/M)$. Q. E. D.

REFERNCES

(1). R. Baer: Abelian Groups which are direct summands of every containing group, Proc. Amer. Math. Soc., 46 (1940) 800-806.

(2). J. Goldhaber & G. Ehrlich: Algebra, The Macmillan Company.

(3). B. Eckmann and A. Schopf: Über Injektive Moduln, Archi. der Math., 4 (1953) 75-78.

(4). I. Kaplansky: Fields and Rings, the University of Chicago Press.

(5). J. Fraleigh: A First Course in Abstract Algebra, Addison-wesley Publishing Company.

(6). A. Rosenberg and D. Zelinsky: Finiteness of the Injective Hull, Math. Z., 70 (1959) 372-380.

(7). E. Matlis: Injective Modules over Prufer Rings, Nagoya Math. J., 15 (1959) 57-69.

(8). G. D. Findlay and J. Lambek: A Generalized Ring of Quotients I, II, Canad. Math. Bull. 2 (1958) 77-85, 155-167.