Villamayor, O. E.
Osaka J. Math.
4 (1967), 161-171

SEPARABLE ALGEBRAS AND GALOIS EXTENSIONS

O.E. VILLAMAYOR

(Received September 14, 1966)

0. In [4] Serre defines an unramified revetement as an affine morphism φ of varieties satisfying some particular conditions (see §1) and he shows that every unramified revetement can be obtained as a quotient of a Galois revetement by the action of a subgroup of the Galois group.

Trying to extend these results to arbitrary preschemas we can translate everything to a pure algebraic setting.

In §1 we prove that the conditions for unramified revetement are equivalent to the separability of the associated rings for each affine open set. In §2 we give some complements to Galois theory (as developed in [2] and [6]) and in §3 we prove that every separable algebra can be functorially embedded in a Galois extension.

The results of §2 are either obvious consequences of [6] or they belong to a forthcoming paper by the same authors.

The results of §3 generalize similar results by Auslander and Goldman ([1], Th. A. 7).

1.

Let $\varphi: Y \to X$ be a morphism of preschemas. If θ_Y, θ_X are the structure sheaves of Y, X respectively, then $\varphi_*(\theta_Y)$ is a sheaf $\mathfrak{A}$ of θ_X-algebras.

According to Serre [4] we will say that φ is an unramified revetement if

1) φ is an affine morphism.
2) $\mathfrak{A}$ is a projective finite θ_X-module.
3) For each $P \in X$, rad $\mathfrak{A}_P = \mathfrak{A}_P$. rad $(\theta_X)_P$.
4) $\mathfrak{A}_P/\text{rad } \mathfrak{A}_P$ is separable over $(\theta_X)_P/\text{rad } (\theta_X)_P$.

If U is an affine open set in X, $\varphi^{-1}(U)$ is affine in Y by 1). We want to prove that, if R is the ring of U (i.e., $\{U.\ \theta_X | U\}$ is isomorphic to Spec R and the associated canonical sheaf) and S is the ring of $\varphi^{-1}(U)$, the previous conditions are equivalent to S being a separable projective R-algebra.

This gives the translation from the geometric to an algebraic problem. We will not come back to Geometry, and we will leave as an exercise to the willing

reader to retranslate the results back.

Notation. If ν is a prime ideal in R we shall call R_ν the localizations of R at ν; for every R-module M (resp. R-algebra A) call $M_\nu = M \otimes_R R_\nu$ (resp. $A_\nu = A \otimes_R R_\nu$).

Lemma 1. *Let I be an ideal in a commutative ring R. Then $I \subset \operatorname{rad} R$ if for every f.g. R-module N, $IN = N \Rightarrow N = 0$.*

Proof. If $I \subseteq \operatorname{rad} R$, let N be a f.g. module with $IN = N$, then $N = 0$ by Nakayama's lemma. If $I \not\subseteq \operatorname{rad} R$, there is a maximal ideal $\nu \subseteq R$ with $I + \nu = R$, hence $R/\nu \neq 0$ and $I \cdot R/\nu = R/\nu$.

Lemma 2. *Let S be a finite commutative R-algebra. Then $S \cdot \operatorname{rad} R \subseteq \operatorname{rad} S$.*

Proof. If N is f.g. S-module, then it is a f.g. R-module. Since

$$(S \cdot \operatorname{rad} R)\, N = \operatorname{rad} R \cdot N, \quad \text{then}$$
$$(S \cdot \operatorname{rad} R)\, N = N \Rightarrow \operatorname{rad} R \cdot N = N \Rightarrow N = 0\,.$$

so by lemma 1:

$$S \cdot \operatorname{rad} R \subseteq \operatorname{rad} S\,.$$

Corollary. *If S is a finite R-algebra with R local, then S is semilocal.*

Lemma 3. *Let A be a ring (not necessarily commutative), R a subring contained in the center of A (with the same unit) and M a finitely generated finitely presented A-module. Then, if M_ν is A_ν-projective for every $\nu \subseteq R$, then M is A-projective.*

Proof. Since M is assumed finitely presented, then M is projective if it is flat.

From the canonical isomorphism

$$[\operatorname{Tor}_1^A(M, N)] \otimes_R R_\nu = \operatorname{Tor}_1^{A_\nu}(M, N)$$

and the fact that M_ν is A_ν-flat, we get $(\operatorname{Tor}_1^A(M, N) \otimes_R R_\nu = 0$ for every maximal ideal ν of R. Hence $\operatorname{Tor}_i^A(M, N) = 0$ for all N and M is A-flat.

Corollary. *Let A be an R-algebra of finite type (R a commutative ring). If for every maximal ideal ν of R, A_ν is separable over R_ν, then A is separable over R.*

Proof. A separable over R means A is a projective $A \otimes_R A^0$-module. R is contained in the center of $A \otimes_R A^0$ and $A_\nu \otimes_{R_\nu} A_\nu^0 = (A \otimes_R A)_\nu$. On the other

hand, A of finte type implies A has finite $A\otimes A^0$-presentation. Then lemma 3 applies.

Lemma 4. *Let S be a commutative finite R-algebra with R local. If for every maximal ideal v of S, S_v is separable over R, then S is separable over R.*

Proof. Consider the inclusion $\varepsilon_1: S\to S\otimes_R S$ given by $\varepsilon_1(x)=x\otimes 1$. By hypothesis S_v is $S_v\otimes S_v$-projective. Since $S_v\otimes S_v$ is $S_v\otimes S$-flat, by a change of rings argument we get S_v is $S_v\otimes S$-flat. Since $\varepsilon_1(S)$ is a subring with the same unit in $S\otimes S$, lemma 3 gives the desired result.

Theorem 1. *Let S be a commutative finite R-algebra. Then S is separable over R if and only if for every maximal ideal v of R the following conditions hold*:

a) $rad\ S_v=S_v\cdot rad\ R_v$

b) $S_v/rad\ S_v$ *is separable over* $R_v/rad\ R_v$.

The necessity of the conditions is an obvious consequence of the fact that S separable over R implies

$$S_v/S_v \text{ rad } R_v \text{ is separable over } R_v/\text{rad } R_v\,.$$

Let us prove the sufficiency:

i) Because of the corollary of lemma 3, it is enough to prove that S_v is separable over R_v for each v, hence we may assume R is local (so $R=R_v$).

Then S is semilocal. If for every maximal ideal α of S, S_α is separable, then S is separable over R (lemma 4).

So we may assume S is local, rad $S=S$ rad R and $S/\text{rad } S$ is a separable field extension of $R/\text{rad } R$, hence there is an element $\bar{c}\in S/\text{rad } S$ such that $\{1, \bar{c}, \cdots, \bar{c}^{n-1}\}$ is a basis of $S/\text{rad } S$ (as a vector space) over $R/\text{rad } R$.

If $c\in S$ maps onto $\bar{c}$, then $\{1, c, \cdots, c^{n-1}\}$ is a set of generators of S as an R-module (by using Nakayama's lemma). Hence c^n is a linear combination of $1, c, \cdots, c^{n-1}$ so

$$c^n+a_{n-1}c^{n-1}+\cdots+a_0=0$$

By reducing modulo the radical, we get

$$\bar{c}^n+\bar{a}_{n-1}\bar{c}^{n-1}+\cdots+\bar{a}_0=0$$

and, by counting dimensions, we see this is the minimal equation (hence irreducible and separable) of $\bar{c}$ over $R/\text{rad } R$. We will call $\bar{F}$ the image of $F\in S[x]$ in $(S/\text{rad } S)[x]$. Since $\overline{\frac{dF}{dX}}(c)=\frac{d\bar{F}}{dX}(\bar{c})$ then $\frac{d\bar{F}}{dX}(\bar{c})\neq 0$ implies that the derivative $\sum_{i=1}^{n} ia_ic^{i-1}$ is invertible in S.

Let $\mu: S\otimes S\to S$ be the map defined by $\mu(x\otimes y)=xy$.

To prove that S is separable over R we will give an explicit form for the idempotent $e\in S\otimes S$ such that $\mu(e)=1$ and $(1\otimes c-c\otimes 1)e=0$ (this last condition implies Ker $\mu\cdot e=0$ since Ker μ is, in this case, the ideal generated by $1\otimes c-c\otimes 1$).

We had $X^n+a_{n-1}X^{n-1}+\cdots+a_0=F(X)\in R[X]$ with a root c in S: hence, in $S[X]$ we have $F(X)=(X-c)G(X)$. If we call $F'(X)$ the formal derivative, then $F'(X)=(X-c)G'(X)+G(X)$, so $F'(c)=G(c)$ is invertible in S.

Define the maps ε_0, $\varepsilon_1: S\to S\otimes S$ by $\varepsilon_0(a)=1\otimes a$, $\varepsilon_1(a)=a\otimes 1$ and call ε_0, ε_1 also the induced maps $S[X]\to(S\otimes S)X$. Now, both $\varepsilon_0(c)$ and $\varepsilon_1(c)$ are roots of $F(X)$ (F had coefficients in R, hence $\varepsilon_0F=\varepsilon_1F$), and applying ε_0 to

$$F(X) = (X-c)G(X) \qquad \text{we get}$$
$$F(X) = (X-\varepsilon_0 c)\cdot(\varepsilon_0 G(X)$$

and
$$F(\varepsilon_1 c) = (\varepsilon_1 c-\varepsilon_0 c)\varepsilon_0 G(\varepsilon_1 c) = 0$$

Since $G(c)$ is invertible in S, so is $\varepsilon_0(G(C))=\varepsilon_0 G(\varepsilon_0 c)$ in $S\otimes S$. Take $e=\dfrac{\varepsilon_0 G(\varepsilon_1 c)}{\varepsilon_0 G(\varepsilon_0 c)}$, hence, using the fact that $\mu\varepsilon_i=\mathrm{id.}$, $\mu(e)=1$ and $(c\otimes 1-1\otimes c)e=(\varepsilon_1 c-\varepsilon_0 c)e=0$.

2. Galois extensions

Notation. If V is separable over R the unique idempotent e such that $1-e$ generates Ker $\mu: V\otimes_R V\to V$ will be called e (V/R).

DEFINITION. Let T be a commutative ring with 1, R a subring (with the same unit). Then T is called a *Galois extension of R with Galois group G* if G is a finite group of automorphismes of T such that $R=T^G$ (i.e. R is the set of elements of T invariant under every $\sigma\in G$) and T is projective and separable over R.

It follows that T is finite over R ([3], [6]).

Since we assume T is separable over R, then Ker $\mu: T\otimes_R T\to T$ is generated by an idempotent $1-e$. Call $e_\sigma=(1\otimes\sigma)(e)$ and $f_\sigma=\mu(e_\sigma)$.

Lemma 5. *Let T be Galois over R. Then $f_1=1$ and f_σ is an idempotent of T such that $\sigma\neq 1\Rightarrow f_\sigma\neq 1$*

For every $x\in S$, $(1\otimes x)e=(x\otimes 1)e$ and applying $1\otimes\sigma$ we obtain $(1\otimes\sigma(x))e_\sigma=(x\otimes 1)e_\sigma$, hence (applying μ)

$$\sigma(x)f_\sigma = x\cdot f_\sigma, \qquad (x-\sigma(x))\cdot f_\sigma = 0$$

hence, $f_\sigma=1$ implies $x=\sigma(x)$, $\forall x$, so $\sigma=1$. Since $e^2=e$, $(1\otimes\sigma)e^2=e_\sigma^2=(1\otimes\sigma)e=e_\sigma$ and (μ is a ring homomorphism) $f_\sigma^2=f_\sigma$.

Corollary. *If T is Galois over R and T has no idempotents, other than* 0 *and* 1, *then* $f_\sigma=\delta_{1,\sigma}$ (*Kronecker* δ). In this case, T is Galois in the sense of [2], which we will call *C-H-R-Galois.*

Corollary. *If T is Galois over R with Galois group G and T has noi. p. other than* 0 *and* 1, *then* $[G:1]=[T:R]$.

Since ([1], Th. 1. 3) $T\otimes_R T$ is T-isomorphic to a direct sum of as many copies of T as the order of G, T being faithfully flat over R implies the corollary.

Lemma 6. *Let T be Galois over R with Galois group G. Assume R has no i.p. other than* 0 *and* 1. *Then* $[G:1]\geqslant[T:R]$.

Since T is finite over R, a simple rank argument shows that T has only a finite number of idempotents. Let $m_1, \cdots, m_k$ be the minimal idempotents of T. If we consider Σm_j for all j such that there is a $\sigma\in G$ with $\sigma(Tm_1)=Tm_j$, then Σm_j is an i.p. in R, hence $\Sigma m_j=1$; so, all Tm_j are mutually isomorphic and G acts transitively in the set $\{m_1, \cdots, m_k\}$. Call $U=Tm_1$

Then $$r = [T: R] = k\cdot[U: R]$$

Call $$n = [G: 1]$$

Since G is transitive over $\{m_1, \cdots, m_k\}$, choose $\sigma_1=\mathrm{id}$, $\sigma_2, \cdots, \sigma_k$ such that $\sigma_i(m_1)=m_i$

If we call $G_1=\{\sigma\in G; \sigma(m_1)=m_1\}$ then every element of G can be uniquely written as $\tau\sigma_i(\tau\in G_1)$ for some i (in fact, if $\alpha(m_1)=m_i$, then $\sigma_i^{-1}\alpha\in G_1$). Then

$$[G: 1] = k[G_1: 1]\,, \qquad [G_1: 1] = n/k\,.$$

Call $G^1=G_1|U$, hence there is an epimorphism $\Phi: G_1\to G^1$ and $[G^1: 1]\leqslant n/k$ (=only if Φ is an isomorphism). Writing $T=Tm_1\oplus\cdots\oplus Tm_k$ and identifying Tm_1 with Tm_i through σ_i, any $t\subset T$ can be written $t=(a_1, \cdots, a_k)$, $a_i\in U$.

$$t\in T^G = R \quad \text{if} \quad a_i = a_1 \quad \text{and} \quad \tau(a_1) = a_1 \forall\tau \quad \text{in} \quad G_1\,,$$

hence $U^{G^1}=R$.

Since U has no i.p. then $[G^1:1]=[U:R]$, $[G^1:1]=r/k$ hence $r/k\leqslant n/k$ and $r\leqslant n$.

Lemma 7. *Let T be Galois over R with Galois group G. Assume R has no i.p. other than* 0 *and* 1. *If* $[G:1]=[T:R]$ *then* $f_\sigma=0$ *for every* $\sigma\neq 1$.

According to the proof of the previous lemma, $n=r$ if and only if $\Phi: G_1\to G^1$ is an isomorphism. If we call G_i the set of $\sigma\in G$ such that $\sigma(m_i)=m_i$, then σ_i (the one we chose in that proof) gives an isomorphism $G_1\to G_i$. Φ being an isomorphism implies (now for every i) that from $\sigma(m_i)=m_i$, $\sigma\neq\mathrm{id}$ follows $\sigma|Tm_i\neq\mathrm{id}$.

Since U is separable over R, let $e(U/R)=\Sigma x_j\otimes y_j$, then $e(S/R)=\Sigma_{i,j}\sigma_i(x_j)m_i\otimes\sigma_i(y_j)m_i$ and $f_\sigma=\Sigma_{j,i}\sigma_i(x_j)m_i\otimes\sigma\sigma_i(y_j)\sigma(m_i)$, hence, if $\sigma(m_i)\neq m_i$ the m_i's being minimal i.p., then $m_i\sigma(m_i)=0$, so, the only remaining terms are those in which $m_i=\sigma(m_i)$. But $\sigma\neq 1$ implies $\sigma\mid Tm_i\neq 1$ because Φ is an isomorphism, hence $\Sigma_j x_j\sigma(y_j)=0$ and we are done.

Theorem 2. *Let T be Galois over R with group G. If T has a rank over R and $[G:1]=[T:R]$, then $f_\sigma=0$ $\forall\sigma$ in G.*

If $(f_\sigma)_\nu=0$ for every $T_\nu=T\otimes_R R_\nu$ when ν runs over all maximal ideals in R, then $f_\sigma=0$. But R_ν, being a local ring, has no i.p. other than 0 and 1. Separability, projectivity and rank are preserved under localization, and G induces G_ν as R_ν-autos of T_ν in the obvious way. We have to show that ${T_\nu}^{G_\nu}=R_\nu$ and $[G_\nu:1]=[T_\nu:R_\nu]=[T:R]$ and then apply the previous lemma. Obviously $R_\nu\subseteq {T_\nu}^{G_\nu}$.

Let $x\in {T_\nu}^{G_\nu}$, then $x=y/r$ $y\in T$, $r\in R$, $r\notin\nu$, and $\sigma_\nu(x)=\sigma(y)/r$, hence $\sigma_\nu(x)=x$ implies the existence of $k\in R$, $k\notin\nu$ such that $k(\sigma(y)-y)=0$ (in T). Since G is finite we may assume k independent of σ, so $\sigma(ky)-ky=0$ or $z=ky\in T^G=R$, and $y=z/k\in R_\nu$. Since the map $G\to G_\nu$ is an epimorphism then $[G_\nu:1]\leqslant[G:1]=[T:R]$. But the lemma shows that $[G_\nu:1]\geqslant[T_\nu:R_\nu]=[T:R]$. Hence $[G_\nu:1]=[T_\nu:R_\nu]$ and lemma 7 applies, hence $(f_\sigma)_\nu=0$ and we are done.

3. Embedding of a separable algebra into a Galois extension

Let S be a separable projective faithful R-algebra with rank $[S:R]=n$. We want to embed S in an algebra T, Galois over R with Galois group (isomorphic to) the symmetric group $\mathfrak{S}_n$ (the group of permutations of $\{a_1,\cdots,a_n\}$) with rank $[T:R]=n!$ such that $T^{\mathfrak{S}_{n-1}}=S$ where we consider $\mathfrak{S}_{n-1}$ embedded into $\mathfrak{S}_n$ as the subgroup leaving fixed the element a_1.

The n different inclusions ε_j of $\mathfrak{S}_{n-1}$ will also give isomorphic copies of S.

Call, for simplicity, $S^i=S\otimes S\otimes\cdots\otimes S$ i times, and consider the sequence

$$R\longrightarrow S\underset{\varepsilon_i}{\overset{\varepsilon_0}{\rightrightarrows}} S^2\;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow}\; S^3\cdots$$

where $\varepsilon_i\colon S^k\to S^{k+1}$ $(0\leqslant i\leqslant k)$ is defined by

$$\varepsilon_i(s_1\otimes\cdots\otimes s_k)=s_1\otimes\cdots\otimes s_i\otimes 1\otimes s_{i+1}\otimes\cdots\otimes s_k$$

Define now maps $\mu_{ij}\colon S^k\to S^{k-1}$ by

$$\mu_{ij}(s_1\otimes\cdots\otimes s_k)=s_1\otimes\cdots\underset{\text{place } i}{\otimes s_is_j}\otimes\cdots\otimes\hat{s}_j\otimes\cdots\otimes s_k\quad(1\leqslant i,j\leqslant k,\ i\neq j)$$

call $N^k=\bigcap\operatorname{Ker}\mu_{ij}\subseteq S^k$.

The algebra T we want is N^n and $\mathfrak{S}_n$ acts on T induced by the permutations

of the factors in S^n.

Since μ_{12} is the only μ from $S^2 \to S$, we have the splitting exact sequence

$$0 \longrightarrow N^2 \longrightarrow S^2 \xrightarrow{\mu} S \longrightarrow 0$$

and $[S:R]=[S^2:S]=n$ implies $[N^2:S]=n-1$ and N^2 is a projective separable S-algebra.

Let us prove first that N^r is projective separable R-algebra with rank and $[N^r:R]=\Pi_i^{r-1}{}_0(n-i)=n!/(n-r)!$. Induction. For $r=2$, $[N^2:S]=n-1$ implies $[N^2:R]=n(n-1)$, the remaining condition being obvious consequences of the previous remark.

Consider $\varepsilon_0: S^{r-1} \to S^r$, then $N^r \subseteq S \otimes N^{r-1}$ (since $S \otimes N^{r-1} = \cap \operatorname{Ker} \mu_{ij}$ $(i \neq 1)$) and μ_{1j} induce $\bar{\mu}_j: S \otimes N^{r-1} \to N^{r-1}$. It is immediately verified that $N^r = \cap \operatorname{Ker} \bar{\mu}_j$ and we get the exact sequence

$$0 \longrightarrow N^r \longrightarrow S \otimes N^{r-1} \xrightarrow{\bar{\mu}} \Sigma \oplus N^{r-1}$$

where $$\bar{\mu} = \Sigma_{h=2}^{r} \bar{\mu}_h .$$

If we prove $\bar{\mu}$ is an epimorphism, since $[S:R]=n$, $[N^{r-1}:R]=\Pi_0^{r-2}(n-i)$ and the sequence splits, then

$$[N^r:R] = n[N^{r-1}:R] - (r-1)[N^{r-1}:R] = \Pi_0^{r-1}(n-i)$$

Since each μ_{ij} is a multiplication map

$$S^k = S^{k-1} \otimes_{S^{k-2}} S^{k-1} \longrightarrow S^{k-1} ,$$

S^{k-1} separable over S^{k-2} implies $\operatorname{Ker} \mu_{ij}$ is an ideal in S^k generated by an idempotent $1-e_{ij}$.

If $$e = \Sigma x_h \otimes y_h = e(S/R) , \quad \text{then}$$

$$e_{ij} = \Sigma_h 1 \otimes \cdots \otimes \overset{i}{x_h} \otimes \cdots \otimes \overset{j}{y_h} \otimes \cdots \otimes 1 .$$

Hence $N^k = \cap \operatorname{Ker} \mu_{ij}$ is the ideal generated by $E_k = \Pi (1-e_{ij})$. Hence N^k is a projective separable R-algebra.

We have $\bar{\mu}_j(e_{1j})=1$, $\bar{\mu}_h(e_{1j})=e_{h-1,j-1}$ if $h \neq j$. Since the map $\bar{\mu}$ is an S^{r-1} homomorphism, to see it is onto it is enough to check the S^{r-1}-generators of ΣN^{r-1} are in $\operatorname{Im} \mu$. Those generators are

$$F_j = (0, \cdots, 0, \underset{j}{E_{r-1}}, 0, \cdots, 0) .$$

Let $$k_j = e_{1j} \cdot \varepsilon_0 E_{r-1} , \qquad \text{then}$$

$$\bar{\mu}(k_j) = (\bar{\mu}_2(k_j), \cdots, \bar{\mu}_t(k_j)) \qquad \text{but}$$

$$\bar{\mu}_j(k_j) = \bar{\mu}_j(e_{1j}) \bar{\mu}_j(\varepsilon_0 E_{r-1}) = E_{r-1}$$

$$\bar{\mu}_h(k_j) = e_{h-1,j-1} \cdot E_{r-1} = 0 \text{ (if } h \neq i)$$

hence $\bar{\mu}(k_j) = F_j$ for every j.

We want to prove now that T contains a copy of S.

Lemma 8. *The map $S \to N^2 \subseteq S^2$ defined by $x \to (x \otimes 1)(1-e)$ is a monomorphism.*

Proof. Let $(s \otimes 1)(1-e)=0$. Since e is invariant under the permutation $x \otimes y \to y \otimes x$, then $(1 \otimes s)(1-e)=0$, hence $(s \otimes 1 - 1 \otimes s)(1-e)=0$ and $(s \otimes 1 - 1 \otimes s)e=0$ imply $s \otimes 1 = 1 \otimes s$, hence $s \in R$.

If $k \in R$ and $k(1-e)=0$, we have, for every

$$x \in S \quad (1 \otimes x)k = (1 \otimes x)ke = k(1 \otimes x)e$$
$$(x \otimes 1)ke = (x \otimes 1)k$$

hence $1 \otimes k \cdot x = k \cdot x \otimes 1$ so $kx \in R$ and $kS \subseteq R$. Since S is a projective R-algebra of rank $n \neq 1$ then $S = R \oplus C$ (as R-modules), C projective with rank and not zero, then $kS \subseteq R$ implies $kC=0$. Localizing, C_ν is free hence $k_\nu C_\nu = 0$ implies $k_\nu = 0$ hence $k=0$.

Lemma 9. *The maps $\Gamma_{i,t}: N^i \to N^{i+t}$ defined by*

$$\Gamma_{i,t}(x_1 \otimes \cdots \otimes x_t) = (x_1 \otimes \cdots \otimes x_t \otimes 1 \otimes \cdots \otimes 1)E_{i+t}$$

are monomorphisms.

We already proved the lemma in the particular case $S = N^1 \to N^2$. Since $(E_j \otimes 1)E_{j+1} = E_{j+1}$, it will be enough to prove the lemma for $t=1$.

Let $V = N^2 = \operatorname{Ker} \mu$, $\mu: S^2 \to S$, and call $V^r = V \otimes_S \cdots \otimes_S V$. We have already seen that V is a projective faithful separable S-algebra with rank and $[V: S] = n-1$.

Repeating the process explained for S as an R-algebra to V as an S-algebra, call $\tilde{\mu}_{ij}$ the corresponding multiplication maps

$$V^r \longrightarrow V^{r-1} \qquad \text{and} \qquad \tilde{N}^r = \bigcap \operatorname{Ker} \tilde{\mu}_{ij}\,.$$

we have monomorphisms

$\theta^r: V^r \to S^{r+1}$ defined by the composition $V^r \to S^2 \otimes_S \cdots \otimes_S S^2 \to S^{r+1}$ where each S^2 is an S-module by the action on the first factor, the second map being the canonical isomorphism. Hence

$$\begin{array}{ccc} \theta_r: & V^r & \longrightarrow S^{r-1} \\ & \tilde{\mu}_{ij}\downarrow & \downarrow \mu_{i+1,j+1} \\ \theta_{r-1}: & V^{r-1} & \longrightarrow S^r \end{array}$$

commutes. The μ_{ij}'s not appearing in this way are all zero on V^r, then $\tilde{N}^r=N^{r+1}$.

In fact, θ^r identifies V^r with $\bigcap_j \operatorname{Ker}\mu_{ij}$, and, $\theta^{r-1}\tilde{\mu}_{ij}=\mu_{i+1,j+1}\theta^r$ shows that θ^r induces the isomorphism $\tilde{N}^r\to N^{r+1}$.

We complete the proof of the lemma by induction over $[S:R]$. If $[S:R]=1$ then $S=R$ and everything works.

Let $[S:R]=n$ and assume the result is true for every case $[U:W]<n$. Hence the lemma holds for V as an S-algebra, i.e., $\tilde{N}^i\to\tilde{N}^{i+1}$ is monic, and so is $N^{i+1}\to N^{i+2}$. We need then to check $S=N^1\to N^2$, which was already proved.

We have then obtained a chain of algebras,

$$R\subset S\subset N^2\subset\cdots\subset N^n$$

where N^i is a projective faithful separable N^{i-1}-algebra with rank, $[N^i:N^{i-1}]=n-i+1$ (It also follows that $N^M=0$ for $M>n$).

Let $\mathfrak{S}_n$ be the symmetric group acting as permutations of the factors of S^n. Since N^n is invariant under $\mathfrak{S}_n$ and it is generated by a unique idempotent E_n, then E_n is invariant under $\mathfrak{S}_n$. $\mathfrak{S}_n$ induces a group of automorphisms of N^n.

In the chain of algebras we considered before, R was identified with RE_n in N^n.

Since $N^n=\tilde{N}^{n-1}$ (corresponding to the construction for $V=N^2$ as an S-algebra) the group $\mathfrak{S}_{n-1}$, acting on N^n as an S-algebra corresponds to the subgroup of $\mathfrak{S}_n$ of those permutations which leave fixed the first factor. In the same way, $\mathfrak{S}_j$ acts leaving fixed the first $n-j$ factors.

We want to prove $(N^n)^{\mathfrak{S}_n}=R$. Induction on $[S:R]$.

If $[S:R]=1$, $R=S=N^1$ and we have nothing to prove.

Assume it is true for $[S:R]<n$. Then it is true for V over S, hence

$$(\tilde{N}^{n-1})^{\mathfrak{S}_{n-1}}=S\,,\qquad\text{or}\qquad (N^n)^{\mathfrak{S}_{n-1}}=S\,.$$

Assume $\alpha\in N^n$ is invariant under $\mathfrak{S}_n$.

In particular, it is invariant under $\mathfrak{S}_{n-1}$, and our induction hypothesis implies $\alpha\in\operatorname{Im}(S)$.

We have two maps $S\to V$, say θ_1, θ_2 where $\theta_i(s)=\varepsilon_i(s)E_2$.
Call $\lambda\colon V\to N^n$ the inclusion defined above. Then

$$\alpha=\lambda\cdot\theta_1(s)\quad\text{for some}\quad s\in S$$

Let σ be the permutation interchanging the two first factors. Then, easy computations show that $\sigma(\alpha)=\lambda\cdot\theta_0(s)$, λ being a monomorphism, $\alpha=\sigma(\alpha)$ implies $\theta_1(s)=\theta_0(s)$, hence $[\varepsilon_0(s)-\varepsilon_1(s)]E_2=0$ but $E_2=1-e$, $[\varepsilon_0(s)-\varepsilon_1(s)]e=0$ shows that $\varepsilon_0(s)=\varepsilon_1(s)$ in S^2. Hence $s\in R$ and we are done. The fact that $[N^n:R]=[\mathfrak{S}_n:1]$ shows that N^n is Galois in the sense of CHR.

Throughout this section we have been assuming that S has a rank over R. If not, R splits in a finite number of direct summands R_K over which S_K has rank K(*). By embedding each S_K into the corresponding N_K^K, then $N=\Sigma_K \oplus N_K^K$ will be Galois over R with group $\Pi \mathfrak{S}_K$ (direct product in which only the factors $\mathfrak{S}_K$ for which $R_K \neq 0$ intervene).

In this case, N is Galois in the sense defined in this paper but not in that of C-H-R, any more.

4. Universality

Suppose now S has no proper idempotents. We have, as before $R \subset S \subset T$, T obtained by the previous construction.

Let $h_1, \cdots, h_r$ be the minimal idempotents in T. Call $W_i = Th_i$, then all W_i are S-isomorphic. Since the maps $R \to Rh_i$ and $S \to Sh_i$ are isomorphisms, then W_i is a Galois extension of both R and S.

We want to prove:

Theorem 3. *If S has no proper i.p., and X is a Galois extension of R containing S, there is an isomorphic copy W of W_i in X such that $R \subset S \subseteq W \subseteq X$, i.e., W_i is the Galois envelope of S over R.*

So, let X be a Galois extension of R containing S. If X has proper idempotents, let $h_1, \cdots, h_e$ the minimal ones, $X = \Sigma\, Xh_i$ and all $Y_i = Xh_i$ are mutually isomorphic. By choosing isomorphisms $Y_1 \xrightarrow{\lambda_i} Y_i$ we obtain a subalgebra Y of X, isomorphic to each Y_i, by taking the elements $(y, \lambda_2(y), \cdots, \lambda_e(y))$ in $\Sigma Y_i = X$.

We will prove that Y contains W, isomorphic to each W_i.

Since Y_i is a direct summand in X, then Y_i (hence Y) is Galois over R [6]. Since Y has no i.p., $[G(Y/R):G(Y/S)]=n$ (§2), hence $G(Y/R)$ induces exactly n different R-isomorphisms of S into Y, say $\theta_1 = \mathrm{id}, \theta_2, \cdots, \theta_n$.

Define a map $\alpha: S^n \to Y$ by

$$\alpha(s_1 \otimes \cdots \otimes s_n) = \theta_1(s_1) \cdots \theta_n(s_n) .$$

Let $\bar{S}$ be the subalgebra of Y generated by the copies of S. Hence α induces an epimorphism $\bar{\alpha}: S^n \to \bar{S}$. Now, we had

$$T = S^n \cdot E , \qquad E = \Pi(1 - e_{ij}) , \qquad \text{and}$$
$$(1 \otimes 1 \otimes \cdots \otimes \underset{i}{x} \otimes 1 \otimes \cdots \otimes 1) e_{ij} = (1 \otimes \cdots \otimes \underset{j}{x} \otimes \cdots \otimes 1) e_{ij} ,$$

so applying α we get, to every $x \in S$,

* This is an immediate consequence of [5] Prop. 4 and the fact that S is a finitely generated projective R-module.

$$\theta_i(x)\alpha(e_{ij}) = \theta_j(x)\alpha(e_{ij})$$

but e_{ij} is an i.p. in $\bar{S}$, contained in Y, and Y has no i.p., hence

$$\alpha(e_{ij}) = 0.1\,,$$

but θ_i being different than θ_j, the previous equation shows $\alpha(e_{ij})\neq 1$, then

$$\alpha(E) = 1\,, \quad \text{and} \quad \bar{\alpha}(E) = 1\,, \quad \bar{\alpha}(1-E) = 0\,.$$

Hence α induces an epimorphism α_1: $T\to\bar{S}$.

Since $T=\Sigma Th_i$, and α_1 is a ring homomorphism, $\alpha_1(h_i)$ is an idempotent in $\bar{S}$, hence 0 or 1, α_1 being an epimorphism implies $\alpha_1(h_i)=1$ for some i, hence $\alpha_1(1-h_i)=\alpha_1(\Sigma_{j\neq i}h_j)=0$ and α_1 induces an epimorphism α_2: $Th_i\to\bar{S}$, which combined with the isomorphism $W\to Th_i$ gives $W\to\bar{S}$.

But α_2 being an epimorphism shows that $\bar{S}$ is R-separable. Since Y is R-projective, then Y is $\bar{S}$-projective and $\bar{S}$ is an $\bar{S}$-direct summand in Y, hence an R-direct summand and $\bar{S}$ is R-projective.

But W being R-separable and $\bar{S}$ R-projective imply $\bar{S}$ is W-projective, hence Ker α_2 is generated by an i.p.; since W has no proper i.p. and $\alpha_2\neq 0$, then Ker $\alpha_2=0$, and α_2 is an isomorphism.

REMARK. The result extends easily to the case R has a finite number of idempotents.

UNIVERSIDAD DE BUENOS AIRES

References

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

[2] S. Chase, D. Harrison and A. Rosenberg: *Galois theory and cohomology of commutative rings,* Mem. Amer. Math. Soc. **52** (1965).

[3] T. Nagahara: *A note on Galois theory of commutative rings,* to appear.

[4] J.P. Serre: Espaces fibrés algébriques, Sém. C. Chevalley, 1958 (Anneaux de Chow et Applications).

[5] J.P. Serre: *Modules projectifs et espaces fibrés à fibre vectorielle,* Sém. P. Dubreil, M.L. Dubreil-Jacotin et C. Pisot, 1958, Exp. 23.

[6] O.E. Villamayor and D. Zelinsky: *Galois theory for rings with finitely many idempotents,* to appear in Nagoya Math. J.