SPLITTING RING OF A MONIC SEPARABLE POLYNOMIAL

STUART SUI SHENG WANG
In this short note we prove that if \( S = R[x] = R[X]/(f(X)) \)
is separable over \( R \), where \( f(X) \) is a monic polynomial over \( R \),
then the embedding set up by Auslander and Goldman is the
same as the splitting ring of \( f \) over \( R \) constructed by Barnard.

Throughout, the terms “ring”, “algebra”, and “ring homomorphism”
are to be interpreted as in the category of commutative rings with
identity. \( S \) is an algebra over the ring \( R \), \( f(X) \) is a monic polynomial of
degree \( n \) over \( R \), \( d_i \) is the discriminant of \( f \), \( Z_n \), \( W_i \) \( (1 \leq i \leq n) \) are
indeterminates over \( R \), \( G \) is the symmetric group on \( n \) symbols, and \( \epsilon(\sigma) \)
is the signature of the permutation \( \sigma \).

Auslander and Goldman [1, Theorem A.7, p. 399] show that if \( S \) is
separable over \( R \) such that \( S \) is free of rank \( n \) as a module over \( R \), then \( S \)
can be embedded into a Galois extension \( \Omega \) of \( R \) with group \( G \). Their \( \Omega \)
is defined as follows: Let \( \Gamma = \otimes^n S \) denote the \( n \)-fold tensor product of \( S \)
over \( R \), \( E = \Lambda^n S \) denote the \( n \)-th exterior power of \( S \) over \( R \), \( \pi: \otimes^n S \to \Lambda^n S \) be the natural \((R \text{-module}) \) homomorphism, \( I \) be the
\( R \)-module conductor (\( \ker \pi \)) : \((\otimes^n S)\), (so \( I \) is an ideal of \( \otimes^n S \) and is also
an \( R \)-submodule of \( \ker \pi \)), and define \( \Omega = (\otimes^n S)/I \). The group \( G \) acts
on \( \otimes^n S \) by permuting the \( n \) factors. Since \( \pi_\sigma(\xi) = \epsilon(\sigma) \pi(\xi) \)
for \( \xi \in \otimes^n S \) and \( \sigma \in G \), \( \ker \pi \) is stable under the action of \( G \), hence so is
\( I \). Thus \( G \) acts on \( \Omega \). Since \( \Lambda^n S \approx \otimes^n S/\ker \pi \) is a free \( R \)-module (of
rank 1), \( R \cap \ker \pi = 0 \), so that \( R \cap I = 0 \), and thus the restriction of the
map \( \Gamma \to \Omega = \Gamma/I \) to \( R \) is injective, i.e., \( \Omega \) contains \( R \). For \( 1 \leq i \leq n \), let
\( p_i : S \to \otimes^n S \) be the \( R \)-algebra homomorphism defined by \( p_i(s) = \)
\( 1 \otimes \cdots \otimes 1 \otimes s \otimes 1 \otimes \cdots \otimes 1 \) (the \( s \) occurring in the \( i \)-th place). Then it
follows from the properties of the exterior algebra that for all \( s \in S \),

\[
(*) \quad p_i(s) + \cdots + p_n(s) - \text{trace}_{S/R}(\bar{s}) \in I
\]

where \( \bar{s} \) denotes the \( R \)-endomorphism of \( S \) defined by multiplication by
\( s \). Assume furthermore \( S \) is separable over \( R \), then \( t = \text{trace}_{S/R} \) is
nondegenerate ([1, Proposition A.4, p. 397]). It follows from \( (*) \) and the
non-degeneracy of \( t \) that the composite of the \( R \)-algebra homomor-
phisms \( S \to \Gamma \to \Omega \) gives an imbedding of \( S \) as an \( R \)-algebra into \( \Omega \).
Then it can be shown that \( \Omega \) is a Galois extension of \( R \) with group \( G \)
([1, line 14 of p. 400 to line 18 of p. 402]).
On the other hand, Barnard [2, §5, pp. 285–289] constructs a splitting ring $R_f$ for a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ of degree $n$ over $R$. More specifically,

$$R_f = R[z_1, \ldots, z_n]$$

$$= R[Z_n, \cdots, Z_n]/(e_1 + a_{n-1}, e_2 - a_{n-2}, \ldots, e_n + (-1)^{n-1}a_0)$$

where $e_i$ ($1 \leq i \leq n$) is the elementary symmetric polynomial of degree $i$ in the indeterminates $Z_1, \cdots, Z_n$. The ring $R_f$ is characterized by the following universal property: the polynomial $f$ factors into the product of $n$ linear factors over $R_f$, $f(X) = \prod_{i=1}^{n}(X - z_i)$. And if $A$ is an $R$-algebra over which $f$ factors into the product of $n$ linear factors, $f(X) = \prod_{i=1}^{n}(X - a_i)$, then there is an $R$-algebra homomorphism $R_f \rightarrow A$ which maps $z_i$ to $a_i$ for $i = 1, \ldots, n$. As usual, such an $R_f$ is unique up to isomorphism. The ring $R_f$ contains $R$, is a free $R$-module of rank $n!$ and $G$ acts on $R_f$ by permuting the $z_i$'s. Moreover, $R_f$ contains $R[x] = R[X]/(f(X))$ as an $R$-subalgebra. It is also shown that $R_f$ is a Galois extension of $R$ with group $G$ if and only if $\prod_{i \neq j} (z_i - z_j)$ is a unit in $R$.

However, a moment's reflection will convince one that $\prod_{i \neq j} (z_i - z_j)$ is $d_f$ up to a sign. Recall $d_f$, the discriminant of $f$, is defined to be the discriminant of the basis $1, x, \cdots, x^{n-1}$ of $R[x]$ with respect to $R$, i.e., the determinant of the $n \times n$ matrix $(\text{trace}_{R[x]/R}(x^i x^j)) 1 \leq i \leq n 1 \leq j \leq n$.

For the remainder of the note, $S$ will be $R[x] = R[X]/(f(X))$ and will be assumed to be separable over $R$ or equivalently $[5]$ $d_f$ is a unit in $R$.

We will show that there is a $\varphi : \Omega \rightarrow R_f$ which is both an $R$-algebra and a $G$-module homomorphism. To establish this, let us first observe that there is an $R$-algebra isomorphism

$$\otimes^n S \approx R[W_1, \cdots, W_n]/(f(W_1), \cdots, f(W_n))$$

where for $g(x) \in S = R[x]$, $p_i(g(x))$ goes to the coset of $g(W_i)$ ($1 \leq i \leq n$). Here $p_n$ as before, denotes the $i$th injection: $S \rightarrow \otimes^n S$. On the other hand, there is another description of $I$. Put $x_i = x^{i-1}, t = \text{trace}_{S/R}$, and let the $n \times n$ matrix $(\lambda_{ij})$ be the adjoint matrix of $(t(x_i x_j))$; let

$$y_j = (\lambda_{j1} x_1 + \lambda_{j2} x_2 + \cdots + \lambda_{jn} x_n) d_f^{-1} \quad (1 \leq j \leq n).$$

Then $t(x_i y_j) = \delta_{ij} \quad (1 \leq i, j \leq n)$ [5]. By $\alpha(\xi)$ will be meant the (contravariant) skew-symmetrization of $\xi$, i.e., $\alpha(\xi) = \sum_{\sigma \in S} \varepsilon(\sigma) \sigma(\xi)$ if $\xi \in \otimes^n S$. Then $I$ is precisely the principal ideal generated by
\( \alpha(x_1 \otimes \cdots \otimes x_n) \alpha(y_1 \otimes \cdots \otimes y_n) - 1 \otimes \cdots \otimes 1 \) [1, p. 401]. Let \( s_1, \cdots, s_n \in S \); then \( \alpha(s_1 \otimes \cdots \otimes s_n) = \det(p_i(s_i)) \). This may be verified by expanding as an alternating sum of \( n! \) terms; these terms are precisely those in the sum \( \Sigma_{\sigma \in \mathcal{S}} \epsilon(\sigma) \sigma(s_1 \otimes \cdots \otimes s_n) \) [1, p. 401]. Accordingly \( \alpha(x_1 \otimes \cdots \otimes x_n) = \det(p_i(x_i)) \) and \( \alpha(y_1 \otimes \cdots \otimes y_n) = \det(p_i(y_i)) = d_i^{n-1} \det(p_i(x_i)) \) by taking \( \det(\lambda_i) = d_i \) into account. Hence \( I \) is the principal ideal generated by \( (\det(p_i(x_i)))^2 - d_i \). If follows that the image of \( I \) in \( R[W_1, \cdots, W_n] \), under the aforementioned isomorphism \( \otimes^n S \cong R[W_1, \cdots, W_n]/(f(W_1), \cdots, f(W_n)) \), is the principal ideal generated by \( [\det(W_i^{-1})]^2 - d_i \). Note, however, it is well-known that \( \det(W_i^{-1}) \), a so-called Vandermonde determinant of the sequence \( (W_1, \cdots, W_n) \), has the value \( \prod_{i>j}(W_i - W_j) \). Consequently, this map induces an isomorphism

\[ \Omega \cong R[W_1, \cdots, W_n]/\left\langle f(W_1), \cdots, f(W_n), d_i - \left( \prod_{i>j}(W_i - W_j) \right)^2 \right\rangle \]

and therefore, since \( f(z_1) = 0, \cdots, f(z_n) = 0, d_i = (\prod_{i>j}(z_i - z_j))^2 \), there is an \( R \)-algebra homomorphism \( \varphi: \Omega \to R_f \) which takes the coset of \( W_i \) to \( z_i \) \((1 \leq i \leq n)\). Obviously such an \( \varphi \) preserves the \( G \)-action. Therefore \( \Omega \cong R_f \) by [3, Theorem 3.4, p.12]. This establishes our assertion.

**Remarks.** (1) As a matter of fact, we have also proved the following proposition: If \( S \) is separable over \( R \), then the surjective \( R \)-algebra homomorphism from \( R[w_1, \cdots, w_n] = R[W_1, \cdots, W_n]/(f(W_1), \cdots, f(W_n), d_i - (\prod_{i>j}(W_i - W_j))^2) \) to \( R_f = R[z_1, \cdots, z_n] \) is an isomorphism. This is not necessarily true if \( S \) is not separable over \( R \). For example, take \( R \) to be the field of real numbers and \( f(X) = X^2 + 2X + 1 \), then \( R[W_1, W_2]/(f(W_1), f(W_2), (W_2 - W_1)^2) \) has dimension 3 over \( R \) while \( R_f \) has dimension 2 over \( R \).

(2) Recently, Andy Magid has pointed out that the splitting ring constructed by Barnard is the same as the “free splitting ring” constructed by Nagahara in [4, pp. 150-152].

**References**


Received April 28, 1976 and in revised form June 10, 1977.

UNIVERSITY OF OKLAHOMA
NORMAN, OK 73069

*Current address*: DEPARTMENT OF MATHEMATICS
TEXAS TECH UNIVERSITY
LUBBOCK, TX 79409
Mieczyslaw Altman, *General solvability theorems* ........................................... 1
Denise Amar and Eric Amar, *Sur les suites d’interpolation en plusieurs variables* ................................................................. 15
Herbert Stanley Bear, Jr. and Gerald Norman Hile, *Algebras which satisfy a second order linear partial differential equation* .................................................. 21
Marilyn Breen, *Sets in $R^d$ having $(d - 2)$-dimensional kernels* .................. 37
Gavin Brown and William Moran, *Analytic discs in the maximal ideal space of $M(G)$* ................................................................. 45
Ronald P. Brown, *Quadratic forms with prescribed Stiefel-Whitney invariants* ................................................................. 59
Gulbank D. Chakerian and H. Groemer, *On coverings of Euclidean space by convex sets* ................................................................. 77
S. Feigelstock and Z. Schlussel, *Principal ideal and Noetherian groups* ...... 87
Ralph S. Freese and James Bryant Nation, *Projective lattices* .................. 93
Harry Gingold, *Uniqueness of linear boundary value problems for differential systems* ................................................................. 107
John R. Hedstrom and Evan Green Houston, Jr., *Pseudo-valuation domains* ................................................................. 137
William Josephson, *Coallocation between lattices with applications to measure extensions* ................................................................. 149
M. Koskela, *A characterization of non-negative matrix operators on $l^p$ to $l^q$ with $\infty > p \geq q > 1$* ................................................................. 165
Kurt Kreith and Charles Andrew Swanson, *Conjugate points for nonlinear differential equations* ................................................................. 171
Shoji Kyuno, *On prime gamma rings* ................................................................. 185
Alois Andreas Lechicki, *On bounded and subcontinuous multifunctions* .... 191
Roberto Longo, *A simple proof of the existence of modular automorphisms in approximately finite-dimensional von Neumann algebras* ................................................................. 199
Kenneth Millett, *Obstructions to pseudoisotopy implying isotopy for embeddings* ................................................................. 207
William F. Moss and John Piepenbrink, *Positive solutions of elliptic equations* ................................................................. 219
Mitsuru Nakai and Leo Sario, *Duffin’s function and Hadamard’s conjecture* ................................................................. 227
Mohan S. Putcha, *Word equations in some geometric semigroups* .......... 243
Walter Rudin, *Peak-interpolation sets of class $C^1$* ................................................................. 267
Elias Saab, *On the Radon-Nikodým property in a class of locally convex spaces* ................................................................. 281
Stuart Sui Sheng Wang, *Splitting ring of a monic separable polynomial* ...... 293