Pacific Journal of Mathematics

SPLITTING RING OF A MONIC SEPARABLE POLYNOMIAL

STUART SUI SHENG WANG

Vol. 75, No. 1 September 1978

PACIFIC JOURNAL OF MATHEMATICS
Vol. 75, No. 1, 1978

SPLITTING RING OF A MONIC SEPARABLE POLYNOMIAL

STUART SUI-SHENG WANG

In this short note we prove that if $S = R[x] = R[X]/\langle f(X)\rangle$ 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_f is the discriminant of f, Z_i, W_i $(1 \leqq i \leqq n)$ are indeterminates over R, G is the symmetric group on n symbols, and $\epsilon(\sigma)$ is the signature of the permutation σ.

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 Ω of R with group G. Their Ω is defined as follows: Let $\Gamma = \bigotimes^n S$ denote the n-fold tensor product of S over R, $E = \wedge^n S$ denote the n-th exterior power of S over R, $\pi: \bigotimes^n S \to \wedge^n S$ be the natural (R-module) homomorphism, I be the R-module conductor $(\ker \pi)$: $(\bigotimes^n S)$, (so I is an ideal of $\bigotimes^n S$ and is also an R-submodule of $\ker \pi$), and define $\Omega = (\bigotimes^n S)/I$. The group G acts on $\bigotimes^n S$ by permuting the n factors. Since $\pi\sigma(\xi) = \epsilon(\sigma)\pi(\xi)$ for $\xi \in \bigotimes^n S$ and $\sigma \in G$, $\ker \pi$ is stable under the action of G, hence so is I. Thus G acts on Ω. Since $\wedge^n S \approx \bigotimes^n S/\ker \pi$ 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., Ω contains R. For $1 \leq i \leqq n$, let $p_i: S \to \bigotimes^n S$ 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 $s \in S$,

$$(*) \qquad p_1(s) + \cdots + p_n(s) - \mathrm{trace}_{S/R}(\bar{s}) \in I$$

where $\bar{s}$ denotes the R-endomorphism of S defined by multiplication by s. Assume furthermore S is separable over R, then $t = \mathrm{trace}_{S/R}$ is nondegenerate ([**1**, Proposition A.4, p. 397]). It follows from $(*)$ and the non-degeneracy of t that the composite of the R-algebra homomorphisms $S \xrightarrow{p_1} \Gamma \longrightarrow \Omega$ gives an imbedding of S as an R-algebra into Ω. Then it can be shown that Ω 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,

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

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

where e_i $(1 \leqq i \leqq n)$ 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, $f(X) = \Pi_{i=1}^n (X - z_i)$. And if A is an R-algebra over which f factors into the product of n linear factors, $f(X) = \Pi_{i=1}^n (X - a_i)$, then there is an R-algebra homomorphism $R_f \to A$ which maps z_i to a_i for $i = 1, \cdots, n$. 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 $R[x] = R[X]/\langle f(X)\rangle$ as an R-subalgebra. It is also shown that R_f is a Galois extension of R with group G if and only if $\Pi_{i \neq j} (z_i - z_j)$ is a unit in R.

However, a moment's reflection will convince one that $\Pi_{i \neq j} (z_i - z_j)$ 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 $(\text{trace}_{R[x]/R}(x^{i-1}x^{j-1}))$ $1 \leqq i \leqq n$ $1 \leqq j \leqq n$.

For the remainder of the note, S will be $R[x] = R[X]/\langle f(X)\rangle$ 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 $\varphi: \Omega \to R_f$ 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

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

where for $g(x) \in S = R[x]$, $p_i(g(x))$ goes to the coset of $g(W_i)$ $(1 \leqq i \leqq n)$. Here p_i, as before, denotes the ith injection: $S \to \otimes^n S$. 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 (λ_{ij}) be the adjoint matrix of$(t(x_ix_j))$; let

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

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

$$\Omega \approx R[W_1, \cdots, W_n] \Big/ \Big\langle f(W_1), \cdots, f(W_n), d_f - \Big(\prod_{i>j}(W_i - W_j)\Big)^2 \Big\rangle$$

and therefore, since $f(z_1) = 0, \cdots, f(z_n) = 0$, $d_f = (\Pi_{i>j}(z_i - z_j))^2$, there is an R-algebra homomorphism $\varphi: \Omega \to R_f$ which takes the coset of W_i to z_i $(1 \leqq i \leqq n)$. Obviously such an φ preserves the G-action. Therefore $\Omega \approx R_f$ 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 $R[w_1, \cdots, w_n] = R[W_1, \cdots, W_n]/\langle f(W_1), \cdots f(W_n), \quad d_f - (\Pi_{i>j}(W_i - W_j))^2\rangle$ 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 $R[W_1, W_2]/\langle f(W_1), f(W_2), (W_2 - W_1)^2\rangle$ 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

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

2. A. D. Barnard, *Commutative rings with operators* (*Galois theory and ramification*), Proc. London Math. Soc., (3) **28** (1974), 274–290.

3. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc., No. 52 (1965) (third printing 1969), 1–19.

4. T. Nagahara, *On separable polynomials over a commutative ring II*, Math. J. of Okayama Univ., **15** (1971/72), 149–162.

5. S. S. Wang, *Separable algebras and free cubic extensions over commutative rings*, Ph.D. thesis, Cornell University, 1975.

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

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typ ›rm or offset-reproduced (not dittoed), double spaced with large margins. Underline Greek letters in re ierman in green, and script in blue. The first paragraph or two must be capable of being used separately as ʼnopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, hich case they must be identified by author and Journal, rather than by item number. Manuscripts, ıplicate, may be sent to any one of the four editors. Please classify according to the scheme of Math. Review ıdex to Vol. **39**. All other communications should be addressed to the managing editor, or Elaine Bart ʼniversity of California, Los Angeles, California, 90024.

100 reprints are provided free for each article, only if page charges have been substantially pai .dditional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $72. year (6 Vols., 12 issues). Special rate: $36.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should ent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

UBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Printed at Jerusalem Academic Press, POB 2390, Jerusalem, Israel.

Pacific Journal of Mathematics

Vol. 75, No. 1 September, 1978

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