# ON THE INVARIANTS OF THE SPLITTING ALGEBRA

ANDERS THORUP

Department of Mathematical Sciences, University of Copenhagen

**Abstract.** For a given monic polynomial $p(t)$ of degree $n$ over a commutative ring $k$, the *splitting algebra* is the universal $k$-algebra in which $p(t)$ has $n$ roots, or, more precisely, over which $p(t)$ factors,

$$p(t) = (t - \xi_1) \cdots (t - \xi_n).$$

The symmetric group $\mathfrak{S}_r$ for $1 \leq r \leq n$ acts on the splitting algebra by permuting the first $r$ roots $\xi_1, \ldots, \xi_r$. We give a natural, simple condition on the polynomial $p(t)$ that holds if and only if there are only trivial invariants under the actions. In particular, if the condition on $p(t)$ holds then the elements of $k$ are the only invariants under the action of $\mathfrak{S}_n$.

We show that for any $n \geq 2$ there is a polynomial $p(t)$ of degree $n$ for which the splitting algebra contains a nontrivial element invariant under $\mathfrak{S}_n$. The examples violate an assertion by A. D. Barnard from 1974.

**1. Introduction.** Consider commutative algebras over a fixed commutative ring $k \neq 0$. Fix a monic polynomial $p(t)$ of degree $n \geq 1$ with coefficients in $k$:

$$p(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_1 t + a_n, \quad a_0 = 1. \tag{1.1}$$

For $r = 0, 1, \ldots, n$ let $\mathrm{Split}^r(p) = \mathrm{Split}^r(p/k)$ be the *r'th splitting algebra* of $p(t)$, universal with respect to factorizations,

$$p(t) = (t - \xi_1) \cdots (t - \xi_r)\tilde{p}(t), \tag{1.2}$$

with $r$ factors $t - \xi_j$. In other words, such a factorization exists in $\mathrm{Split}^r(p)[t]$, with elements $\xi_1, \ldots, \xi_r$ in $\mathrm{Split}^r(p)$ and a polynomial $\tilde{p}(t) \in \mathrm{Split}^r(p)[t]$, and if $A$ is any $k$-algebra over which $p(t)$ factors,

$$p(t) = (t - \alpha_1) \cdots (t - \alpha_r)q(t), \tag{1.3}$$

1991 *Mathematics Subject Classification*. 13B25, 13B05.

[1]The author was supported in part by the Danish Natural Science Research Council, grant 21–02–0458.

then there is a unique $k$-algebra homomorphism $\mathrm{Split}^r(p) \to A$ such that $\xi_j \mapsto \alpha_j$ for $j = 1, \dots, r$, and, consequently, $\tilde{p}(t)$ is mapped to $q(t)$. The (*complete*) *splitting algebra* of $p(t)$ is obtained when $r = n$; then $\tilde{p}(t)$ in (1.2) and $q(t)$ in (1.3) are equal to 1.

Clearly, the $r$'th splitting algebra is generated by the $r$ universal roots $\xi_1, \dots, \xi_r$ in (1.2). It follows from the construction of $\mathrm{Split}^r(p)$ in Section 2 that the natural map $\mathrm{Split}^r(p) \to \mathrm{Split}^n(p)$ is an injection, identifying $\mathrm{Split}^r(p)$ with the subalgebra $k[\xi_1, \dots, \xi_r]$ of $\mathrm{Split}^n(p) = k[\xi_1, \dots, \xi_n]$.

Let $\Psi_p$ be the element of $k$ defined as the product $\Psi_p = \prod_{i<j}(\xi_i + \xi_j)$. The product is a symmetric polynomial in the roots $\xi_1, \dots, \xi_n$, and hence $\Psi_p$ a polynomial in the coefficients $a_j$ of $p(t)$. In particular, $\Psi_p \in k$. There is a simple determinantal formula for $\Psi_p$, see Definition4.

It follows from the universal property that the symmetric group $\mathfrak{S}_n$ acts on the complete splitting algebra $\mathrm{Split}^n(p)$ by permuting the roots $\xi_1, \dots, \xi_n$. Obviously, the elements of the algebra $\mathrm{Split}^r(p) = k[\xi_1, \dots, \xi_r]$ are invariant (or fixed) under the action of the subgroup $\mathfrak{S}'_{n-r}$ consisting of permutations in $\mathfrak{S}_n$ fixing the numbers $1, \dots, r$. The main result of this paper is the following characterization, part of Theorem 7.

**Result.** *The invariants are trivial:* $k[\xi_1, \dots, \xi_n]^{\mathfrak{S}'_{n-r}} = k[\xi_1, \dots, \xi_r]$ *for* $r = 0, \dots, n$, *if and only if* $\mathrm{Ann}_k \Psi_p \cap \mathrm{Ann}_k 2 = (0)$.

In particular, the equality $k[\xi_1, \dots, \xi_n]^{\mathfrak{S}_n} = k$ holds if $\mathrm{Ann}_k \Psi_p \cap \mathrm{Ann}_k 2 = (0)$. Barnard [Ba, p. 289] asserted the equality for $n \geq 3$ without any condition on $p(t)$. We show by a counterexample that the general assertion is not true.

Let $p^{(r)}(t)$ be the polynomial $\tilde{p}(t)$ in (1.2). Then the factorization has the form,

$$p(t) = p_r(t)p^{(r)}(t), \quad \text{where } p_r(t) := (t - \xi_1) \dots (t - \xi_r). \tag{1.4}$$

Let $K_r = \mathrm{Fact}^r(p)$ be the $k$-subalgebra of $\mathrm{Split}^n(p)$ generated by the elementary symmetric polynomials in $\xi_1, \dots, \xi_r$, or, equivalently, by the coefficients of $p_r(t)$. Then both polynomials $p^{(r)}(t)$ and $p_r(t)$ have coefficients in $K_r$. Under the condition $\mathrm{Ann}_k \Psi_p \cap \mathrm{Ann}_k 2 = (0)$ on $p(t)$, we prove in Proposition 11 that the elements of $K_r$ are the only invariants of the action of $\mathfrak{S}_r$ on the $r$'th splitting algebra, that is, $k[\xi_1, \dots, \xi_r]^{\mathfrak{S}_r} = K_r$.

**2. Construction.** A construction of the complete splitting algebra is given in [Ba, p. 286], in [Bo, p. IV.67, §5], and in [PZ, p. 30]. We recall here the recursive construction of the intermediate algebras $S_r := \mathrm{Split}^r(p)$ for $r = 0, \dots, n$:

Obviously, $S_0 = \mathrm{Split}^0(p) = k$. For $r = 1$, the equation (1.3) holds if and only if $\alpha_1 \in A$ is a root of $p(t)$. The universal algebra in which $p(t)$ has a root is obtained by *adjoining formally a root* of $p(t)$:

$$S_1 = \mathrm{Split}^1(p) := k[x]/(p(x)), \qquad \xi_1 := (x \mod p(t)).$$

Assume that $S_r := \mathrm{Split}^r(p/k)$ has been defined in general, for $r < n$, with a factorization (1.2). Then, clearly, we obtain $S_{r+1}$ by adjoining formally a root of $p^{(r)}(t)$, or, equivalently, as the $r$'th splitting algebra of $p^{(1)}(t)$ over $S_1$:

$$\mathrm{Split}^{r+1}(p/k) := \mathrm{Split}^1(p^{(r)}/S_r) = \mathrm{Split}^r(p^{(1)}/S_1).$$

**3. Proposition.** *The monomials* $\xi_1^{i_1}\xi_2^{i_2}\cdots\xi_r^{i_r}$ *where* $0 \le i_\nu \le n-\nu$ *for* $\nu = 1,\dots,r$ *form a* $k$*-basis for the* $r$*'th splitting algebra* $\mathrm{Split}^r(p)$. *In particular,* $\mathrm{Split}^r(p)$ *is free of rank* $n(n-1)\cdots(n-r+1)$ *as a* $k$*-module, and* $\mathrm{Split}^n(p)$ *is free of rank* $n!$.

*Proof.* The assertion follows by induction on $r$ from the recursive definition of $\mathrm{Split}^r(p)$.

*Note.* It is an easy consequence of the Proposition that the roots $\xi_1,\dots,\xi_n$ are $n$ different elements in $\mathrm{Split}^n(p)$ except when $n = 2$, $a_1 = 0$, and $2 = 0$ in $k$.

**4. Definition.** Consider in $\mathrm{Split}^n(p) = k[\xi_1,\dots,\xi_n]$ the Vandermonde determinant $\Delta_p$,

$$\Delta_p = \prod_{i<j}(\xi_i - \xi_j) = \sum_{\sigma\in\mathfrak{S}_n}(\mathrm{sign}\,\sigma)\,\sigma\left(\xi_1^{n-1}\xi_2^{n-2}\cdots\xi_{n-1}\right),$$

and the two elements $\Psi_p$ and $\mathrm{Discr}_p$,

$$\Psi_p = \prod_{i<j}(\xi_i + \xi_j) \quad \text{and} \quad \mathrm{Discr}_p = \prod_{i<j}(\xi_i - \xi_j)^2.$$

The element $\mathrm{Discr}_p = \Delta_p^2$ is of course the *discriminant* of $p(t)$.

The elements $\Psi_p$ and $\mathrm{Discr}_p$ are symmetric polynomials in the roots $\xi_1,\dots,\xi_n$, and consequently can be expressed as polynomials in the coefficients of $p(t)$. In particular, the elements $\Psi_p$ and $\mathrm{Discr}_p$ belong to $k$.

It is well known that $\Psi_p$, as a polynomial in the $\xi_i$, is a Schur polynomial, see [Mc, Example 7, p. 46] or [Mu, formula 339 p. 334]. As a polynomial in the elementary symmetric polynomials $e_j$ it is the determinant $\Psi = \det(e_{2i-j})$, see [Mc, Formula (3.5), p. 41]. In terms of the coefficients $a_i = (-1)^i e_i$ of $p(t)$ we obtain the expression $\Psi_p = (-1)^{n(n-1)/2}\det(a_{2i-j})$,

$$\Psi_p = (-1)^{n(n-1)/2}\begin{vmatrix} a_0 & 0 & 0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & 0 & \cdots & 0 \\ a_4 & a_3 & a_2 & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{2n-2} & a_{2n-3} & a_{2n-4} & a_{2n-3} & \cdots & a_{n-1} \end{vmatrix}.$$

In particular, in low degrees: For $n = 1$: $\Psi = 1$, for $n = 2$: $\Psi = -a_1$, for $n = 3$: $\Psi = a_3 - a_1a_2$, and for $n = 4$: $\Psi = a_1a_2a_3 - a_1^2a_4 - a_3^2$.

**5. Lemma.** *Assume for $n \geq 2$ that $F \in k[\xi_1]$ is $\mathfrak{S}_2$-invariant. Then:*
(1) *If $n \geq 3$, then $F \in k$.*
(2) *If $n = 2$, then $F = b\xi_1 + c$, with $b, c \in k$ and $2b = \Psi_p b = 0$.*

*Proof.* Let $\tau$ be the non-trivial permutation in $\mathfrak{S}_2$, acting on the second splitting algebra $k[\xi_1, \xi_2]$ by interchanging $\xi_1$ and $\xi_2$. By assumption, $F \in k[\xi_1]$ and $\tau F = F$. Write $F$ in the form $F = Q(\xi_1)$, where $Q \in k[x]$ is a polynomial of degree less than $n$, say $Q = bx^{n-1} + cx^{n-2} + \cdots$. Then $Q(\xi_2) = Q(\xi_1)$. So the polynomial $Q(x) - Q(\xi_1)$ in $k[\xi_1][x]$ has $\xi_2$ as a root. Hence $Q(x) - Q(\xi_1)$ is a multiple of $p^{(1)}(x)$. As $p^{(1)}(x)$ is monic of degree $n-1$ it follows by comparing the degrees and the leading coefficients that

$$Q(x) - Q(\xi_1) = bp^{(1)}(x). \tag{5.1}$$

After multiplication by $x - \xi_1$, we obtain the following equation in $k[\xi_1][x]$:

$$\big(Q(x) - Q(\xi_1)\big)(x - \xi_1) = bp(x). \tag{5.2}$$

Compare the coefficients of $x^{n-1}$ in the equation. If $n \geq 3$ we obtain the equation $-b\xi_1 + c = ba_1$. In particular, $b\xi_1 \in k$, and hence $b = 0$. From (5.1) we conclude that the polynomial $Q(x)$ is a constant. Hence $F = Q(\xi_1)$ belongs to $k$. Thus Part (1) has been proved.

The case $n = 2$ is easily treated directly. Alternatively we may use (5.2). Equating the coefficients of $x$ gives the equation $-2b\xi_1 = ba_1$. Here $a_1 = -(\xi_1 + \xi_2) = -\Psi_p$, and hence $2b\xi_1 = \Psi_p b$. As $\xi_1, 1$ are linearly independent over $k$, it follows that $2b = \Psi_p b = 0$. Thus Part (2) has been proved.

**6. Proposition.** *Assume for $n > r \geq 1$ that $F \in k[\xi_1, \ldots, \xi_r]$ is $\mathfrak{S}_{r+1}$-invariant. Then:*
(1) *If $r \leq n-2$ then $F \in k$.*
(2) *If $r = n - 1$ then $2F \in k$ and $\Psi_p F \in k$.*

*Proof.* Set $S_j := k[\xi_1, \ldots, \xi_j]$. Then $S_j = S_{j-1}[\xi_j]$ is the first splitting algebra of $p^{(j-1)}(t)$ over $S_{j-1}$. The degree of $p^{(j-1)}$ is $n - j + 1$, and hence at least 3 if $j \leq n - 2$.

Therefore, under the assumptions in Part (1), it follows by repeated application Lemma 5(1) that $F \in S_{j-1}$ for $j = r, \ldots, 1$. With $j = 1$ it follows that $F \in k$.

For Part (2), note first that the assertion for $n = 2$ follows from Lemma 5(2). Proceed by induction on $n \geq 3$. Note that $\mathrm{Split}^n(p)$ is the complete splitting algebra of $p^{(1)}(t)$ over $k[\xi_1]$. Clearly

$$\Psi_p = \Phi \Psi_{p^{(1)}} \quad \text{where } \Phi := \prod\nolimits_{1<j\leq n} (\xi_1 + \xi_j).$$

Moreover, $\Phi \in k[\xi_1]$; in fact $\Phi = (-1)^{n-1} p^{(1)}(-\xi_1)$. By induction, $2F$ and $\Psi_{p^{(1)}} F$ belong to $k[\xi_1]$. So both products $2F$ and $\Psi_p F$ belong to $k[\xi_1]$. As both products are $\mathfrak{S}_n$-invariant, it follows from Lemma 6(1) that they belong to $k$.

**7. Theorem.** *Let* $S = \mathrm{Split}^n(p/k) = k[\xi_1, \dots, \xi_n]$ *be the complete splitting algebra of* $p(t)$*. Assume that* $n \geq 2$*. Then the following conditions on* $p(t)$ *are equivalent:*

(i) $\mathrm{Ann}_k \mathrm{Discr}_p \cap \mathrm{Ann}_k 2 = (0)$.
(ii) $\mathrm{Ann}_k \Psi_p \cap \mathrm{Ann}_k 2 = (0)$.
(iii) $S^{\mathfrak{S}'_2} = k[\xi_1, \dots, \xi_{n-2}]$.
(iv) $S^{\mathfrak{S}'_{n-r}} = k[\xi_1, \dots, \xi_r]$ *for* $r = 0, 1, \dots, n-2$*, where* $\mathfrak{S}'_{n-r}$ *denotes the subgroup of permutations in* $\mathfrak{S}_n$ *fixing the numbers* $1, \dots, r$.

*Proof.* For an element $F \in S$ and a subset $V \subseteq S$ denote by $F|V$ the restriction to $V$ of multiplication by $F$. Consider with $I := \mathrm{Ann}_S 2$ the following three conditions:

$$\text{(i*)}\quad \mathrm{Ker}\,\mathrm{Discr}_p\,|I = (0), \qquad \text{(ii*)}\quad \mathrm{Ker}\,\Psi_p|I = (0), \qquad \text{(iii*)}\quad \mathrm{Ker}(\xi_{n-1}+\xi_n)|I = (0).$$

The algebra $S$ is free as a $k$-module and the elements $\Psi_p$ and $\mathrm{Discr}_p$ belong $k$. Hence (i) is equivalent to (i*) and (ii) is equivalent to (ii*). Set $S_{r-2} = k[\xi_1, \dots, \xi_{r-2}]$. Then $S$ is the complete splitting algebra over $k[\xi_1, \dots, \xi_{n-1}]$ of the degree 2-polynomial $p^{(n-2)}$. By Lemma 5(2), (iii) holds if and only if $\mathrm{Ann}_{S_{n-2}} 2 \cap \mathrm{Ann}_{S_{n-2}}(\xi_{n-1} + \xi_n) = (0)$. Again, as $S$ is free over $S_{n-2}$, the latter condition holds if and only if (iii*) holds.

Since $I = \mathrm{Ann}_S 2$ it follows that $\Psi_p|I = \Delta_p|I$. Hence $\mathrm{Discr}_p\,|I = (\Psi_p|I)^2$. Consequently $\Psi_p|I$ is injective if and only if $\mathrm{Discr}_p\,|I$ is injective. Hence (i*) $\Longleftrightarrow$ (ii*).

Again, $\Psi_p|I$ is the product of the factors $(\xi_i+\xi_j)|I$ for $i < j$. Hence, if $\Psi|I$ is injective, then the factor $(\xi_{n-1}+\xi_n)|I$ is injective. Assume conversely that the factor $(\xi_{n-1}+\xi_n)|I$ is injective. Then, since the group $\mathfrak{S}_n$ acts by automorphisms of $S$, every factor $(\xi_i+\xi_j)|I$ (with $i < j$) is injective, and hence the product $\Psi|I$ is injective. Hence (ii*) $\Longleftrightarrow$ (iii*).

Obviously (iii) is part of the conditions in (iv), and hence (iv)$\Rightarrow$(iii). Clearly, to finish the proof it suffices to show that (ii) implies that the equality in (iv) for $r = 0$ holds. So assume that $F \in S$ is $\mathfrak{S}_n$-invariant. Then, by Proposition 6 we have the relations $2F = 0$ and $\Psi_p F = 0$. The relations mean that if $F$ is expanded in terms of the basis in Proposition 3 then all coefficients to base elements different from 1 are annihilated by 2 and by $\Psi_p$. Therefore, if (ii) holds then all these coefficients vanish, that is, $F \in k$.

**8. Corollary.** *If any of the three elements:* 2*, or* $\mathrm{Discr}_p$*, or* $\Psi_p$*, is a non-zero divisor in* $k$*, then the conditions of the Theorem hold. In particular, then*

$$k[\xi_1, \dots, \xi_n]^{\mathfrak{S}_n} = k. \tag{8.1}$$

*Proof.* Clearly, under the given assumptions either (i) or (ii) of the Theorem holds. Hence (iv) holds, and in particular (8.1) which is the special case $r = 0$ of (iv) holds.

**9. Notes.** The results in the Corollary for the elements 2 and $\mathrm{Discr}_p$ were proved by Pohst and Zassenhaus [PZ, (2.18d), p. 46 and (3.6), p. 49] and, with a different proof, by Laksov and Ekedahl [EL, Theorem 5.1 and Remark 5.3, p. 13–14]. Pohst and Zassenhaus also proved the assertion in Proposition 6(2), but with $\Psi_p$ replaced by $\mathrm{Discr}_p$.

It was asserted by Barnard [Ba, Proposition 4, p. 289] that the equality (8.1) holds for all $n > 2$. However, a simple counterexample shows that the assertion cannot hold in the stated generality: Consider the splitting algebra of the polynomial $p(t) = t^n$ ($n \geq 2$). It is easy to see, by induction on $r = 1, \dots, n-2$, that $\xi_1^{n-1} \cdots \xi_r^{n-r} \xi_r = 0$. It follows easily for $\sigma \in \mathfrak{S}_n$ that

$$\sigma\big(\xi_1^{n-1}\xi_2^{n-2}\cdots\xi_{n-1}\big) = (\operatorname{sign}\sigma)\xi_1^{n-1}\xi_2^{n-2}\cdots\xi_{n-1}.$$

Hence for $z \in \mathrm{Ann}_k 2$ the element $z\xi_1^{n-1}\xi_2^{n-2}\cdots\xi_{n-1}$ is invariant, and it is non-trivial if $z \neq 0$. A second family of non-trivial invariants is given in Example 10.

It is an open question, at least to the knowledge of the author, whether the equality (8.1) implies the stronger conditions in Theorem 7.

**10. Example.** A natural idea to construct invariants in $\mathrm{Split}^n(p)$ ($n \geq 2$) is to write the Vandermonde determinant $\Delta_p$ as the difference,

$$\Delta_p = \Delta^+ - \Delta^-, \qquad \Delta^+ = \sum_{\sigma\in\mathfrak{A}_n} \sigma\big(\xi_1^{n-1}\xi_2^{n-2}\cdots\xi_{n-1}\big),$$

where the sum is over all even permutations. Then $\Delta^+$ and $\Delta^-$ are invariant under even permutations and interchanged by odd permutations. In particular, if $z \in k$ then $z\Delta^+$ is invariant under $\mathfrak{S}_n$ if and only if $z$ is in the kernel of multiplication by $\Delta_p$ as a map $k \to S$. But naturally, even if $z \neq 0$ and $z\Delta_p = 0$, it may happen that $z\Delta^+ = 0$.

In particular, assume that $z \in \mathrm{Ann}_k 2$. Then, as noted above, $z\Delta_p = z\Psi_p$, and hence $z\Delta_p^+$ is invariant if and only if $z \in \mathrm{Ann}_k \Psi_p$. For $n = 2$ or $n = 3$ it is easy to see that the invariants of the complete splitting algebra are the elements $c + z\Delta_p^+$ for $c \in k$ and $z \in \mathrm{Ann}_k 2 \cap \mathrm{Ann}_k \Psi_p$.

**11. Proposition.** *Fix $r$ with $1 \leq r \leq n$ and let $K = \mathrm{Fact}^r(p)$ be the $k$-subalgebra of $\mathrm{Split}^n(p)$ generated by the elementary symmetric polynomials in the first $r$ roots $\xi_1, \dots, \xi_r$, or, equivalently, by the coefficients of the polynomial $p_r(t) := (t-\xi_1)\cdots(t-\xi_r)$. Then, in $K[t]$ we have the factorization,*

$$p(t) = p_r(t)\,p^{(r)}(t), \tag{11.1}$$

*of $p(t)$ into two monic factors, the first of degree $r$ and the second of degree $n-r$. Moreover, the $k$-algebra $K$ is universal with respect to this property. Furthermore, the algebra*

$\mathrm{Split}^r(p) = k[\xi_1, \ldots, \xi_r]$ *is the complete splitting algebra of the degree-r polynomial* $p_r(t)$ *over* $K$*:*

$$\mathrm{Split}^r(p/k) = \mathrm{Split}^r(p_r/K). \tag{11.2}$$

*Finally, if the equivalent conditions of Theorem* 7 *hold for* $p(t)$*, then*

$$k[\xi_1, \ldots, \xi_r]^{\mathfrak{S}_r} = K. \tag{11.3}$$

*Proof.* The equation (11.1) is simply (1.2). The polynomial $p_r(t)$ has, by construction, coefficients in $K$. Therefore, by (11.1), so has $p^{(r)}(t)$.

Obviously, the polynomial $p_r(t) \in K[t]$ splits completely over $S_r := k[\xi_1, \ldots, \xi_r]$. To prove (11.2), we verify that the splitting is universal. So assume that $\varphi_0 \colon K \to A$ is an algebra such that $p_r(t)$ factors completely over $A$ with $r$ factors $t - \alpha_j$. Then we obtain in $A[t]$ the factorization (1.3) where $q(t)$ is the image in $A[t]$ of $p^{(r)}(t)$. So, by the universal property of $S_r = \mathrm{Split}^r(p/k)$, there is a unique $k$-algebra homomorphism $\varphi \colon S_r \to A$ such that $\varphi(\xi_j) = \alpha_j$ for $j = 1, \ldots, r$. It remains to prove that $\varphi$ is a map $K$-algebras, that is, $\varphi$ is equal to $\varphi_0$ on the $k$-subalgebra $K$ of $S_r$. The equality results from the fact that under both maps the coefficients of $p_r(t)$ are mapped to the signed elementary symmetric polynomials of the $\alpha_j$. So the two maps agree on the coefficients of $p_r(t)$, and since $K$ is generated as a $k$-algebra by these coefficients, the two maps agree on $K$.

The universal property of $K$ with respect to factorizations $p(t) = \tilde{q}(t)q(t)$ with two factors of degrees $r$ and $n - r$ is proved similarly: Assume that such a factorization exists over a $k$-algebra $A$. Since $K$ is generated by the coefficients of $p_r(t)$ there is at most one $k$-algebra homomorphism $K \to A$ under which $p_r(t)$ is mapped to $\tilde{q}(t)$. To prove the existence, consider the complete splitting algebra $T_r$ of $\tilde{q}(t)$ over $A$. Then there is a $k$-algebra homomorphism $S_r \to T_r$ such that the $\xi_j$ are mapped to the roots of $\tilde{q}(t)$. In particular, $p_r(t)$ is mapped to $\tilde{q}(t)$. As $K$ is generated by the coefficients of $p_r(t)$, and the coefficients of $\tilde{q}(t)$ belong to $A$, we obtain the map $K \to A$ as the restriction of the map $S_r \to T_r$.

To prove the final assertion, consider the equivalent conditions of Theorem 7. Assume that they hold for $p(t)$. Note that the factors defining the product $\Psi_{p_r}$ are also factors of $\Psi_p$. Therefore,

$$\mathrm{Ann}_K\, 2 \cap \mathrm{Ann}_K\, \Psi_{p_r} \subseteq \mathrm{Ann}_{S_r}\, 2 \cap \mathrm{Ann}_{S_r}\, \Psi_p.$$

Since $S_r$ is free over $k$, condition (ii) for $p(t)$ implies that the right hand intersection is trivial. Therefore the left hand intersection is is trivial, that is, condition (ii) holds for $p_r(t)$ in $K[t]$. Moreover, $k[\xi_1, \ldots, \xi_r]$ is the complete splitting algebra of $p_r(t)$ over $K$ by (11.2). Therefore, by the Theorem, condition (iv) holds for $p_r(t)$; in particular (11.3) holds.

**12. Note.** The algebra $\mathrm{Split}^r(p)$ is free over $k$ of rank $n(n-1)\cdots(n-r+1)$ by construction, and it is free over $K = \mathrm{Fact}^r(p)$ of rank $r!$ by (11.2). We showed in the paper with D. Laksov [LT] that $K = \mathrm{Fact}^r(p)$ is in fact $k$-free of rank $\binom{n}{r}$, generated by suitable Schur polynomials in $\xi_1, \ldots, \xi_r$. The paper describes in addition the connection between splitting algebras and intersection rings of Grassmannians (Schubert Calculus).

## References


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

[Bo] N. Bourbaki, *Éléments de Mathématique, Algèbre, Chapitres 4 à 7*, Masson, Paris, 1981.

[EL] T. Ekedahl and D. Laksov, *Splitting algebras, symmetric polynomials, and Galois theory*, J. Algebra Appl. **4** (2005), 59–75.

[LT] D. Laksov and A. Thorup, *Schubert calculus on Grassmannians and exterior powers*, Indiana Univ. Math. J. **58,** No. 1 (2009), 283–300.

[Mc] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Second Edition, Oxford University Press, Oxford, 1998.

[Mu] T. Muir, *A Treatise on the Theory of Determinants*, Revised and enlarged by W. H. Metzler, Dover, New York, 1960.

[PZ] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1989.