

Elements of Trace 1 in $S[V](L^{-1})$

Clarence Wilkerson *
Wayne State University

If V is an n -dimensional graded F_p -vector space concentrated in degree 2, then the symmetric algebra $S[V]$ may be identified with the F_p -polynomial algebra on n variables of degree 2 and there is a natural action of $GL(V)$ on $S[V]$. The ring of invariants $S[V]^{GL(V)}$ is again a polynomial algebra, generated by the Dickson elements $\{c_{n,i} : 0 \leq i \leq n-1\}$. Let L be the highest dimensional Dickson generator $c_{n,0}$, i.e. just the product in $S[V]$ of the nonzero elements of V . From [Priddy-Wilkerson],

$$S[V]^{GL(V)} \longrightarrow S[V]$$

is a Galois extension in the sense of [Chase-Harrison-Rosenberg] after the inversion of L . As such there is an element in $S[V](L^{-1})$ with trace 1. In other words, there is an element in $S[V]$ which has trace dividing a power of L . In this modular case, an element of trace 1 can not be a constant, so a natural question is to find a formula for an explicit element of trace 1.

These notes sketch a method of computing the trace bilinear form for the extension - a method of computation that makes clear certain choices of elements of trace 1. But first, the definition of one such element:

Theorem I.: For any basis $\langle x_1, \dots, x_n \rangle$ of V , the element

$$DET(x_j^{p^k})_{\substack{1 \leq j \leq n \\ 0 \leq k \leq n-1}} \prod_{0 \leq i \leq n-1} (x_{i+1})^{p^n - p^i - 1} \left(\prod_{v \neq 0} v^{-n} \right)$$

*This research was partially supported by the NSF and the Wayne State Fund.

has trace 1 in $S[V](L^{-1})$.

The first step of the proof of Theorem I. is to relate the irreducible equation of an extension to the computation of the trace. Of course, the trace of a primitive element for the extension is immediate from its minimal equation. However, a method due to Euler computes the trace form from the minimal equation [e.g. Lang, Algebra, p. 213]:

Lemma 2.: If $f(X)$ is an irreducible separable polynomial of degree k over the field F and α is a root of $f(X)$, then the dual basis to $\langle 1, \alpha, \dots, \alpha^{k-1} \rangle$ for $F \langle \alpha \rangle$ over F with respect to the trace bilinear form

$$\langle x, y \rangle = \text{Trace}_{F \langle \alpha \rangle \rightarrow F}(xy)$$

is

$$\langle b_0/f'(\alpha), \dots, b_{k-1}/f'(\alpha) \rangle$$

where

$$f(X)/(X - \alpha) = b_0 + b_1X + \dots + b_{k-1}X^{k-1}.$$

That is,

$$\text{Trace}_{F \langle \alpha \rangle \rightarrow F}(\alpha^i b_j / f'(\alpha)) = \delta_{ij}$$

The problem with applying Euler's method to a given extension is that one may not know an explicit primitive α or its minimal equation. This is the case in our example

$$S[V]^{GL(V)} \longrightarrow S[V].$$

One knows that Dickson's fundamental equation

$$f(X) = \prod_{v \in V} (X - v) = X^{p^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_{n,i} X^{p^{n-i}} = 0$$

valid for all $v \in V$ exhibits this as a splitting ring, but the roots of the fundamental equation are not primitive elements in the sense of field theory.

However, since the trace map is transitive over composite extensions, we can compute the trace from a sequence of extensions, each generated by an element of V . These extensions are not Galois, but the composite of the sequence of extensions is the original Galois extension. The relevant facts and constructions follow below.

Lemma 3.: In a field extension $E \longrightarrow L \longrightarrow K$, if α and β are elements of K and L respectively such that

$$\text{Trace}_{K \rightarrow L}(\alpha) = 1$$

and

$$\text{Trace}_{L \rightarrow E}(\beta) = 1,$$

then

$$\begin{aligned} \text{Trace}_{K \rightarrow E}(\alpha\beta) &= \text{Trace}_{L \rightarrow E}(\text{Trace}_{K \rightarrow L}(\alpha\beta)) = \\ \text{Trace}_{L \rightarrow E}(\beta\text{Trace}_{K \rightarrow L}(\alpha)) &= \text{Trace}_{L \rightarrow E}(\beta) = 1 \end{aligned}$$

In view of these lemmas, the strategy will be to break the extension

$$S[V](L^{-1})^{GL(V)} \longrightarrow S[V](L^{-1})$$

into smaller extensions which are computable. The result is the construction of an explicit element of trace 1.

The Construction:

For the basis $\langle x_1, \dots, x_n \rangle$, define V_i to be the span of $\langle x_1, \dots, x_i \rangle$, and V_0 to be the zero subspace. Let H_i be the subgroup of $GL(V)$ consisting of those elements which act as the identity on V_i . Thus $H_0 = GL(V)$, and $H_n = Id_V$. We can also define polynomials

$$f_i(X) = \prod_{V_i} (X - v)$$

and

$$g_i(X) = f_n(X)/f_i(X) = \prod_{v \notin V_i} (X - v).$$

Clearly, the coefficients of $g_i(X)$ are in the subfield K^{H_i} , where K is the field of fractions of $S[V]$. Also $K^{H_{i+1}} = K^{H_i} \langle x_{i+1} \rangle$

Since x_{i+1} is in the set-theoretic complement of V_i in V , it is a root of $g_i(X)$. Hence Euler's method can be applied to $g_i(X)$. The derivative of $g_i(X)$ is

$$((f_i f'_n - f_n f'_i)/(f_i^2))(x_{i+1}) = f'_n(x_{i+1})/f_i(x_{i+1}) = L/f_i(x_{i+1}).$$

On the other hand, the reduced polynomial is

$$g_i(X)/(X - x_{i+1}) = \prod_{u \notin V_i, u \neq x_{i+1}} (X - u).$$

Thus the leading coefficient $b_{p^n - p^{i-1}}$ is 1. By Euler

$$\text{Trace}_{K^{H_{i+1}} \rightarrow K^{H_i}}((x_{i+1})^{p^n - p^{i-1}} f_i(x_{i+1})/L) = 1.$$

Of course, one could calculate the other $\{b_j\}$ also to obtain different elements of trace 1. For example, b_0 is (up to sign) just the product of the elements of V which are not in V_i or equal to x_{i+1} .

The above construction is valid for $i \in \{1, \dots, n\}$. By the transitivity lemma, the product of the elements constructed has trace 1 in the total extension. By a theorem of E.H. Moore [Moore], the product of the $f_i(x_{i+1})$ is the indicated determinant.

It would be interesting to find the element of $S[V]$ of smallest degree and nonzero trace by this construction. Theorem I. shows directly that the $n - th$ power of L is in the image of the trace, for p odd, and that the $(n - 1) - th$ power of L is in the image of the trace for $p = 2$. Given that $S[V]$ has a module basis over the Dickson algebra of invariants with the largest degree being $2 \sum_{i=0}^{n-1} (p^n - p^i - 1)$, and that the trace form is not identically zero, it must be non-zero on at least one of these module basis elements, and hence this latter number provides an upper bound degree for elements of smallest degree with non-zero trace.

This was a note written in 1984 or so and was TeX'ed in 1986. It was never submitted for publication.