ANNIHILATING POLYNOMIALS, TRACE FORMS AND THE GALOIS NUMBER

Seán McGarraghy

Abstract. We construct examples where an annihilating polynomial produced by considering étale algebras improves on the annihilating polynomial got in [1] by considering Galois numbers.

1. Introduction

Throughout this paper, K is a field of characteristic not equal to 2. The Witt ring $W(K)$ of K is an integral ring and we may consider polynomials with integer coefficients evaluated at an element φ of K. We say a polynomial $p \in \mathbb{Z}$ **annihilates** φ if $p(\varphi) = 0$ in $W(K)$.

During the last decade or so, several examples of annihilating polynomials have appeared in the literature. First, Lewis [7] found a monic polynomial p_n which annihilates any quadratic form of dimension n. At about the same time, Conner [2], using different methods, gave a polynomial q_n of lower degree which annihilates trace forms of dimension n. Beaulieu and Palfrey improved on Conner's results in [1]

Let L/K be a finite separable field extension, let N be the normal closure of L over K, and let $G = \mathrm{Gal}(N/K)$ be the Galois group of N over K. Using an isomorphism between the Burnside ring of finite G-sets and the Grothendieck ring of the category of étale K-algebras (following an approach of Dress) it was shown in

1991 *Mathematics Subject Classification.* 11E81, 12F10, 19A22.

Key words and phrases. Quadratic form, trace form, étale algebra, G-set, Witt ring.

Part-supported by Enterprise Ireland.

[8] that a certain polynomial p_L annihilates $\langle L\rangle$, the class of the trace form of L over K, in the Witt ring $W(K)$. This approach, via étale algebras, enabled one to recover the annihilating polynomials of Conner [2] and of Beaulieu and Palfrey [1] for trace forms of field extensions. Furthermore, it was possible to recover the polynomials of Lewis [7] which annihilate quadratic forms in general.

This paper provides examples which show the results in [8] are an improvement on those in [1]; for a complete exposition of the theory, see [8].

Important terms are defined below. However, the treatment is by no means complete, and for further information on quadratic forms and the Witt ring one should see [9]; for field theory see [4] or [5]; and for background on étale algebras see [6, Ch. V].

2. Quadratic forms and the Witt ring

We define the Witt ring of the field K.

Definition 2.1 A **bilinear form** on a finite-dimensional K-vector space V is a map $b : V \longrightarrow K$ such that:

$$\begin{aligned} b(x+x',y) &= b(x,y)+b(x',y) \\ b(x,y+y') &= b(x,y)+b(x,y') \\ b(\alpha x,y) &= b(x,\alpha y) = \alpha b(x,y) \end{aligned}$$

for all $\alpha \in K$ and all x, x', y, y' in V. We say a bilinear form b is **symmetric** if $b(x,y) = b(y,x)$ for all $x, y \in V$.

Definition 2.2 A **quadratic form** on a finite-dimensional K-vector space V is a map $\varphi : V \longrightarrow K$ such that:
(i) $\varphi(\alpha v) = \alpha^2\varphi(v)$ for all $\alpha \in K$ and all $v \in V$;
(ii) the map : $V \times V \longrightarrow K : (v,w) \mapsto \varphi(v+w) - \varphi(v) - \varphi(w)$ is bilinear.

Remark 2.3 There is a one-one correspondence between symmetric bilinear forms and quadratic forms over K (when K has characteristic not equal to 2).

Definition 2.4 Two bilinear forms $b_1 : V_1 \longrightarrow K$ and $b_2 : V_2 \longrightarrow K$ are said to be **isometric** (written $b_1 \simeq b_2$) if there is a vector space isomorphism $\gamma : V_1 \longrightarrow V_2$ such that $b_2(\gamma(x), \gamma(y)) = b_1(x, y)$ for all $x, y \in V_1$. The **isometry class** of a form is the set of all forms isometric to it.

The **(orthogonal) sum** of forms, $b_1 \perp b_2$ is defined in the obvious way via the direct sum of vector spaces

$$(b_1 \perp b_2)((x_1, x_2)(y_1, y_2)) := b_1(x_1, y_1) + b_2(x_2, y_2).$$

The **(tensor) product** of forms, $b_1 \cdot b_2$ or $b_1 \otimes b_2$ is defined in a natural way on the tensor product of vector spaces $V_1 \otimes_K V_2$:

$$(b_1 \otimes b_2)((x_1 \otimes x_2), (y_1 \otimes y_2)) := b_1(x_1, y_1) b_2(x_2, y_2).$$

Remark 2.5 If b is a bilinear form on V and $\mathcal{B} = \{e_1, \ldots, e_n\}$ is a basis for V, then $B := (b(e_i, e_j)) = (b_{ij})$ is called the matrix of b with respect to the basis $\mathcal{B}$. B is symmetric if and only if b is symmetric. Then, writing

$$x = \sum_{i=1}^{n} e_i x_i, \quad y = \sum_{i=1}^{n} e_i y_i,$$

we have $b(x, y) = x^t B y$. It can easily be shown that, provided $\mathrm{char} K \neq 2$, any symmetric bilinear form b over K can be put in diagonal form (represented by a diagonal matrix) i.e. $b : V \longrightarrow K$ is isometric to a form

$$K^n \longrightarrow K : (x_1, \ldots, x_n) \mapsto a_1 x_1^2 + \cdots + a_n x_n^2$$

for some elements $a_1, \ldots, a_n$ in K. The standard notation for such a diagonal form is

$$\langle a_1, \ldots, a_n \rangle.$$

We write $n \times \langle a \rangle$ for the n-dimensional form $\langle a, a, \ldots, a \rangle$.

Definition 2.6 A bilinear form $b : V \longrightarrow K$ is said to be **isotropic** if $b(v,v) = 0$ for some $v \in V$, $v \neq 0$. Otherwise b is said to be **anisotropic**.

A bilinear form $b : V \longrightarrow K$ is **hyperbolic** if it is isometric to some even-dimensional form

$$\langle 1, -1, 1, -1, \ldots, 1, -1 \rangle.$$

The 2-dimensional form $\langle 1, -1 \rangle$ is called a hyperbolic plane. Thus a hyperbolic form is (isometric to) a sum of hyperbolic planes.

Theorem 2.7 [Witt Cancellation Theorem] If φ, ψ_1 and ψ_2 are symmetric bilinear forms with $\varphi \perp \psi_1 \simeq \varphi \perp \psi_2$, then $\psi_1 \simeq \psi_2$.

Let S be the set of all isometry classes of non-singular symmetric bilinear forms over K. Let the Grothendieck group $G(K)$ be the quotient of the free Abelian group on S by the subgroup generated by elements of the form

$$\{\varphi_1 \perp \varphi_2\} - \{\varphi_1\} - \{\varphi_2\}$$

(where $\{\varphi_i\}$ is the isometry class of the form φ_i, $i = 1, 2$). Then addition in $G(K)$ will correspond to the orthogonal sum of forms, i.e.

$$\{\varphi_1 \perp \varphi_2\} = \{\varphi_1\} + \{\varphi_2\}.$$

It follows from the Witt Cancellation Theorem that the mapping $S \longrightarrow G(K) : \varphi \mapsto \{\varphi\}$ is injective.

We now make $G(K)$ into a ring, the Witt-Grothendieck ring $\widehat{W}(K)$, by using the product of forms. Then $\widehat{W}(K)$ is a commutative ring with identity and it can be shown that the additive subgroup H of $\widehat{W}(K)$ generated by all the hyperbolic forms is an ideal of $\widehat{W}(K)$.

Then the **Witt ring** of K, $W(K)$, is defined to be the quotient ring $\widehat{W}(K)/H$. It can be shown that the set of non-zero elements of $W(K)$ is in one-one correspondence with the set of isometry classes of non-singular anisotropic forms.

Since in characteristic not 2 there is a one-one correspondence between symmetric bilinear forms and quadratic forms, we may also regard the Witt ring as a quotient of the completion of the additive Abelian group of isometry classes of quadratic forms.

3. Étale algebras and G-sets

A finite-dimensional commutative K-algebra A satisfying the equivalent conditions in the following proposition is called **étale**:

Proposition 3.1 *Let A be a finite-dimensional commutative K-algebra. Then the following are equivalent:*
(i) *The symmetric bilinear form $T : A \times A \longrightarrow K$ induced by the trace $T(x, y) = \mathrm{Tr}_{A/K}(xy)$ for all $x, y \in A$ is non-singular;*
(ii) *A is isomorphic to a direct product $L_1 \times \cdots \times L_r$ for some finite separable field extensions $L_1, \ldots, L_r$ of K (and in particular is a direct product of copies of K when K is itself separably closed).*

Definition 3.2 For a finite group G, let $\widehat{G}$ be the **category** of G**-sets**, whose objects are G-sets (finite sets on which G acts by permutations from the left) and whose morphisms are G-maps, i.e. for any two G-sets S and T we have

$$\mathrm{Hom}_G(S, T) = \{\varphi : S \longrightarrow T \mid \varphi(gs) = g\varphi(s) \text{ for all } s \in S, g \in G\}.$$

The set $\Omega(G)^+$ of isomorphism classes of G-sets has the structure of a commutative semi-ring with cancellation (with addition and multiplication being given by disjoint union and Cartesian product respectively of G-sets). We define the **Burnside ring** $\Omega(G)$ to be the ring completion via the usual Grothendieck construction.

For a G-set S, let $[S]$ denote the element in $\Omega(G)$ represented by S.

Henceforth G will be the Galois group of a Galois extension N of K. Let $\textbf{Ét}_{K,N}$ be the category whose objects are étale K-algebras A for which $A \otimes_K N$ is isomorphic to a direct product of a finite number of copies of N, and whose morphisms are K-algebra homomorphisms. Let $\Omega(K, N)$ be the Grothendieck ring of $\textbf{Ét}_{K,N}$.

Remark 3.3 $\Omega(G)$ and $\Omega(K, N)$ are isomorphic because the categories $\widehat{G}$ and $\textbf{Ét}_{K,N}$ are anti-equivalent via the functors

$\widehat{G} \longrightarrow \mathbf{\acute{E}t}_{K,N} : S \mapsto \mathrm{Hom}_G(S,N)$ and $\mathbf{\acute{E}t}_{K,N} \longrightarrow \widehat{G} : A \mapsto \mathrm{Hom}_{K-\mathbf{Alg}}(A,N)$ (under this correspondence simple G-sets–i.e. indecomposable G-sets–correspond to simple algebras i.e. fields, disjoint union of G-sets corresponds to direct product of algebras, and Cartesian product of G-sets corresponds to tensor product of algebras).

Example 3.4 If H is any subgroup of a finite group G, then the set G/H of left cosets $xH \subseteq G$, where $x \in G$, is naturally a G-set, with the action $G \times G/H \longrightarrow G/H$ defined by $(g, xH) \mapsto gxH$.

Definition 3.5 Let S and T be G-sets, and let U be a subgroup of G. Let

$$S^U = \{x \in S : gx = x \text{ for all } g \in U\}.$$

We define

$$\varphi_T(S) = |\mathrm{Hom}_G(T,S)|$$

and

$$\varphi_U(S) = |S^U| = |\mathrm{Hom}_G(G/U,S)|.$$

Remark 3.4 A simple G-set is a set of left cosets G/U with the natural left action, U being a subgroup of G. The G-sets G/U and G/V are isomorphic if and only if U and V are conjugate subgroups. Since $\varphi_U = \varphi_T$ for $T = G/U$ and $\varphi_{T_1 \dot{\cup} T_2} = \varphi_{T_1} \cdot \varphi_{T_2}$, it is enough to work only with the invariants φ_U (resp. the invariants φ_T). We pass freely between notations.

Lemma 3.7 *For any two simple G-sets S and T with $S \cong G/U$ we have*

$$\varphi_S(S) = |Aut_G(S)| = [N_G(U) : U]$$

and

$$\varphi_S(S) \mid \varphi_T(S).$$

4. Annihilating polynomials

Let L/K be a finite separable field extension, with $[L : K] = n$. Then (see [4, Theorem 13.6]) L is a simple extension of K and we may write $L = K(\vartheta_1)$.

Let $f \in K[t]$ be the minimal polynomial of ϑ_1 over K and let N be the normal closure of L over K. Then we may take N to be the splitting field of f over K and we may write f as a product of linear polynomials in $N[t]$, namely,

$$f = \prod_{i=1}^{n} (t - \vartheta_i).$$

Let G be the Galois group $\mathrm{Gal}(N/K)$ of N over K and let H be the subgroup of G whose fixed field is L, by the usual Galois Correspondence.

Definition 4.1 Let E be an extension field of K with $K \leq E \leq N$. We define

$$\varphi_E(L) := \text{ number of components of } E \otimes_K L \text{ isomorphic to } E.$$

Now $E \otimes_K L$ is an étale K-algebra (étale algebras remain étale under extension of scalars) and, denoting by (f) the ideal in $K[t]$ generated by f,

$$E \otimes_K L \ \cong E \otimes_K \frac{K[t]}{(f)} \cong \frac{E[t]}{(f)},$$

which, by the Chinese Remainder Theorem, decomposes into a Cartesian product of field extensions of K, corresponding to the factorization of f into a product of irreducibles in $K[t]$. Since $E[t]/(t - \alpha)$ is isomorphic to E for any $\alpha \in E$, we get, for each root ϑ_i of f in E, a component of $E \otimes_K L$ which is isomorphic to E.

Let $R = \{\vartheta_1, \vartheta_2, \ldots, \vartheta_n\} \subseteq N$. Then basic Galois theory shows that

$$\begin{aligned} \varphi_E(L) = |R \cap E| &= \text{ number of roots of } f \text{ which lie in } E \\ &= \text{ number of monomorphisms } L \longrightarrow E. \end{aligned}$$

We note that if $E \not\subseteq L$, then $\varphi_E(L) = 0$. Also, $\varphi_N(L) = n$, since

$$N \otimes_K L \cong \prod_{i=1}^{n} N.$$

Let V be the subgroup of G with $E = N^V$ (that is, E is the fixed field of V). Then

$$\varphi_E(L) = |(G/H)^V| = |\mathrm{Hom}_G(G/V, G/H)|.$$

By considering an étale K-algebra A as a direct product of separable extensions of K, for any extension E with $K \leq E \leq N$ there is a ring-homomorphism $\varphi_E : \Omega(K, N) \longrightarrow \mathbb{Z}$ where $\varphi_E(A)$ equals the number of components of $E \otimes_K A$ which are isomorphic to E.

Remark 4.2 The isomorphism $\Omega(G) \cong \Omega(K, N)$ in Remark 3.3 allows us to replace φ_U by φ_E and in direct products to let E run through all isomorphism classes of fields E with $K \leq E \leq N$ (since isomorphism classes of subfields correspond to conjugacy classes of subgroups). Then Lemma 3.7 becomes:

Lemma 4.3 *Let $G = Gal(N/K)$, let $H \leq G$ with fixed field L, and let $L \subseteq E$. Then*

$$\varphi_L(L) = |Aut_G(G/H)| = [N_G(H) : H]$$

and

$$\varphi_L(L) \mid \varphi_E(L).$$

Definition 4.4 With K, L and N as above, we define a set,

$$S_L := \{\varphi_E(L) : K \leq E \leq N\}.$$

We also define a polynomial $p_L \in \mathbb{Z}[t]$ by

$$p_L(t) = \prod_{k \in S_L} (t - k).$$

We state without proof the following results from [8].

Theorem 4.5 *The polynomial p_L annihilates $\langle L \rangle$ in the Witt ring $W(K)$, where $\langle L \rangle : L \longrightarrow K$, $\langle L \rangle(x) = Trace_{L/K}(x^2)$ for all $x \in L$.*

Corollary 4.6 *Let the polynomial* $q_L = \prod_{k \in T_L} (t-k)$ *where*

$$T_L := \{k \in S_L : k \equiv n \bmod 2\}.$$

Then q_L *annihilates* $\langle L \rangle$ *in the Witt ring* $W(K)$.

5. Examples

Pierre Conner in 1987 [2] found the first results on annihilating polynomials for trace forms. He showed that the trace form of any separable extension of the field K is annihilated in $W(K)$ by the polynomial

$$p := \prod_{k=0, k \equiv n \bmod 2}^{n} (t-k).$$

(Conner did not publish his result as he believed–correctly–that a better result was possible.) The Beaulieu-Palfrey paper [1] improves on the Conner result and the theorem and corollary above are a further improvement.

Let g be the Galois number of $f \in K[t]$ as defined in [1], that is, g is the smallest natural number j such that any j of the roots of f generate the splitting field N of f. Then $g-1$ is the maximum value of the set $S_L \setminus \{n\}$ where $L := K[t]/(f)$.

The Beaulieu-Palfrey polynomial is

$$(t-n) \prod_{k=0, k \equiv n \bmod 2}^{g-1} (t-k)$$

and q_L divides this, since any g roots generate all of N, that is, there are no fields $E \neq N$ such that $\varphi_E(L) \geq g$.

In many cases q_L is definitely of lower degree than the Beaulieu-Palfrey polynomial. To show this, we construct examples where (with the same notation as above)

$$[N_G(H) : H] > 2.$$

Then by Lemma 4.3, for any field E with $K \leq L \leq E \leq N$ we have

$$2 < \varphi_L(L) \mid \varphi_E(L).$$

Lemma 5.1 *Let p be a prime, let G be a p-group and let H be a proper subgroup of G. Then*

$$H \nsubseteq N_G(H).$$

Example 5.2 Let p be an odd prime and let G be a Sylow p-subgroup of the symmetric group S_{p^2} on p^2 letters.

In particular, taking $p = 3$, we have that $|G| = 81$ and, for any subgroup H of G, 3 divides $[N_G(H) : H] = \varphi_L(L)$ where $L = \mathrm{Fix}H$.

Since Sylow 3-subgroups are conjugate to each other and any 3-subgroup of S_9 is contained in a Sylow 3-subgroup, G will contain a 9-cycle and so act transitively on 9 letters. By the same reasoning G will contain a 3-cycle (but no transposition!) and so by [1, §2, Ex. 2], the Galois number of G is $g = 9 - 2 = 7$. (Since G is a permutation group embedded in S_9, it acts faithfully on 9 letters.)

Now let N/K be a Galois extension with Galois group G as above (results on the inverse Galois problem show that there exist number field extensions with G as Galois group). Let L/K be a field extension of degree 9 such that $K \leq L \leq N$ and the subgroup H of G corresponding to L is not normal in G. (We do not choose $[L : K] = 27$ as then H would be normal in G by 5.1, and so L/K would itself be a normal–and thus Galois–extension.) Then H will be core-free, i.e. contains no normal subgroup of G (if H did contain a normal subgroup, then the action of G on the 9 letters would have a kernel).

Then the possible values of $\varphi_E(L)$ are 0, 3 and $9 = [L : K]$, so in this case we have

$$q_L = (t-3)(t-9) \quad (\text{or possibly } t-9),$$

whereas the Beaulieu-Palfrey polynomial is

$$(t-9) \prod_{\substack{k=0 \\ k \equiv 9 \bmod 2}}^{7-1} (t-k) = (t-1)(t-3)(t-5)(t-9).$$

The essential point here is that the factors in q_L must go up in jumps of 6: a modulo 2 periodicity comes from the even-odd trick in Corollary 4.6 and a modulo 3 periodicity comes from Lemma 4.3. The factors in the Beaulieu-Palfrey polynomial only go up in jumps of 2 and so there are more of them.

Remark 5.3 The same approach may be followed for larger primes than 3, and so there exist examples where the difference in degree between q_L and the Beaulieu-Palfrey polynomial is arbitrarily large.

Since an n-dimensional trace form has diagonalization of the form $n \times \langle 1 \rangle$ for n odd, it is clear it is annihilated by the polynomial $t - n$. A more interesting example would be where the dimension of the trace form is a power of 2. The next example is of this kind.

Example 5.4 Let $p = 2$ and let G be the modular group of order 16,

$$G = \langle \tau, \sigma : \tau^2 = \sigma^8 = 1, \tau\sigma\tau^{-1} = \sigma^5 \rangle.$$

Let H be the subgroup of G generated by τ. Then H is core-free in G because τ is not central in G. Then G acts faithfully on the 8 cosets of H and may be regarded as a subgroup of the symmetric group S_8 on 8 letters, being generated by an 8-cycle σ and an involution τ subject to the relation $\tau\sigma\tau^{-1} = \sigma^5$.

Then

$$\tau\sigma^2\tau^{-1} = (\tau\sigma\tau^{-1})^2 = \sigma^{10} = \sigma^2$$

so τ and σ^2 commute. Thus the normalizer of H in G is generated by τ and σ^2 and so has order 8. So we have that 4 divides $[N_G(H) : H] = \varphi_L(L)$.

By [3, Example 1], the Galois number of G is 5.

As in the previous example, let N/K be a Galois extension with Galois group G. Let L be the fixed field of H, where $K \leq L \leq N$. Then $[L : K] = n = |G|/|H| = 8$.

Thus by the earlier theory the possible values of $\varphi_E(L)$ are 0, 4 and $n = 8$. So we have

$$p_l = q_L = t(t-4)(t-8),$$

whereas the Beaulieu-Palfrey polynomial is

$$(t-8)\prod_{\substack{k=0\\k\equiv 8 \bmod 2}}^{5-1}(t-k) = t(t-2)(t-4)(t-8).$$

Here the factors in $p_L = q_L$ go up in jumps of 4 and there is a factor less than in the Beaulieu-Palfrey polynomial. One may obtain similar examples by considering other suitable 2-subgroups of S_{2^n}, for $n > 3$.

References

[1] P. W. Beaulieu and T. C. Palfrey, *The Galois number*, Math. Ann. **309** (1997), 81-96.

[2] P. E. Conner, *A proof of a conjecture concerning algebraic Witt classes*, preprint, 1987.

[3] M. Epkenhans, *On vanishing of trace forms*, Acta Mathematica et Informatica Universitatis Ostraviensis **6** (1998), 69-85.

[4] D. J. H. Garling, A Course in Galois Theory. Cambridge University Press: Cambridge, 1986.

[5] N. Jacobson, Basic Algebra, II. W. H. Freeman and Company, 1980.

[6] M-A. Knus, A. Merkurjev, M. Rost and J-P. Tignol, The Book of Involutions. Amer. Math. Soc., 1998.

[7] D. W. Lewis, *Witt rings as integral rings*, Inv. Math. **90** (1987), 631-633.

[8] D. W. Lewis and S. McGarraghy, *Annihilating polynomials, étale algebras, trace forms and the Galois number*, Archiv der Math., to appear.

[9] W. Scharlau, Quadratic and Hermitian Forms. Springer-Verlag: Berlin-Heidelberg-Tokyo-New York, 1985.

Seán McGarraghy
Department of Mathematics
University College Dublin
Belfield
Dublin 4
Ireland
e-mail: John.McGarraghy@ucd.ie