Minimum polynomials and the trace form for cyclic extensions

based on work with R. Gow

Rachel Quinlan

July 16, 2009

School of Mathematics, Statistics and Applied Mathematics
National University of Ireland, Galway

NUI Galway
OÉ Gaillimh

Fq9
THE 9TH INTERNATIONAL CONFERENCE ON
FINITE FIELDS AND THEIR APPLICATIONS
UCD, July 13-17 2009

Plan

The trace form for cyclic extensions

Minimum polynomials for subspaces

- Independence of Characters
- Existence

Properties of minimum polynomials

- The case of hyperplanes
- Further remarks on odd degree
- More general properties

The Setup

Let L/K be a cyclic Galois extension of degree n.
Fix a generator σ for the Galois group $\mathrm{Gal}(L/K)$.

The trace function $\mathrm{Tr}_{L/K} : L \longrightarrow K$ is the K-linear mapping defined for $x \in L$ by

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=0}^{n-1} \sigma^i(x).$$

We denote the kernel of the trace function by T.
T is a K-hyperplane of L.
Every K-hyperplane of L is a $L^\times$-translate of T; i.e. can be expressed as aT for some $a \in L^\times$.

The Symmetric Trace Form

The trace form on L is the nondegenerate symmetric K-bilinear form $\tau : L \times L \longrightarrow K$ defined for $x, y \in L$ by

$$\tau(x, y) = \mathrm{Tr}_{L/K}(xy).$$

If U is a K-subspace of L of dimension k, then the orthogonal complement of U with respect to the trace form is the K-subspace of dimension $n - k$ given by

$$\begin{aligned} U^{\perp} &= \{x \in L : \tau(x, u) = 0 \ \forall u \in U\} \\ &= \{x \in L : xu \in T \ \forall u \in U\} \end{aligned}$$

If $\{a_1, \dots, a_k\}$ is a K-basis of U, then

$$U^{\perp} = a_1^{-1} T \cap a_2^{-1} T \cap \cdots \cap a_k^{-1} T.$$

Independence of Characters

Let $p(\sigma)$ be a "polynomial" in the generator σ of $\mathrm{Gal}(L/K)$, with coefficients in L :

$$p(\sigma) = a_k\sigma^k + a_{k-1}\sigma^{k-1} + \cdots + a_1\sigma + a_0.$$

Then $p(\sigma)$ describes a K-linear endomorphism p of L by

$$p(x) := a_k x^{\sigma^k} + \cdots + a_1 x^{\sigma} + a_0 x.$$

Theorem (Artin : Independence of Characters)

The elements of $\mathrm{Gal}(L/K)$ *form a* L*-basis for the endomorphism ring* $\mathrm{End}_K(L)$.

Thus every K-endomorphism of L can be uniquely expressed in the following form, with $a_i \in L$.

$$a_{n-1}\sigma^{n-1} + a_{n-2}\sigma^{n-2} + \cdots + a_1\sigma + a_0.$$

Rank of Endomorphisms

Question Does the representation of $\theta \in \text{End}_k(L)$ as a L-polynomial (of degree at most $n-1$ in σ tell us anything about the properties of θ? For example can we say anything about the *rank* of θ?

Theorem (Gow)

The dimension of the kernel of θ is at most equal to $\deg \theta$.

This means : If U is a K-subspace of L of dimension k, and $p(\sigma)$ is the polynomial representation of an endomorphism which annihiliates U, then $\deg(p(\sigma)) \geq k$.

Rank of Endomorphisms

Question Does the representation of $\theta \in \text{End}_k(L)$ as a L-polynomial (of degree at most $n-1$ in σ tell us anything about the properties of θ? For example can we say anything about the *rank* of θ?

Theorem (Gow)

The dimension of the kernel of θ is at most equal to $\deg \theta$.

This means : If U is a K-subspace of L of dimension k, and $p(\sigma)$ is the polynomial representation of an endomorphism which annihiliates U, then $\deg(p(\sigma)) \geq k$.

Rank of Endomorphisms

Question Does the representation of $\theta \in \mathrm{End}_k(L)$ as a L-polynomial (of degree at most $n-1$ in σ tell us anything about the properties of θ? For example can we say anything about the *rank* of θ?

Theorem (Gow)

The dimension of the kernel of θ is at most equal to $\deg\theta$.

This means : If U is a K-subspace of L of dimension k, and $p(\sigma)$ is the polynomial representation of an endomorphism which annihiliates U, then $\deg(p(\sigma)) \geq k$.

Minimum polynomials

Lemma

If A is a square matrix with entries in L, having the property that each row (except the first) is the image under σ of the previous one, then $\det(A) = 0$ if and only if the elements of the first row of A are linearly dependent over K.

Theorem

Let U be a K-subspace of L of dimension k. Then there exists a polynomial $m_U(\sigma)$ of degree k whose kernel is U.

Proof: Write $U = \langle a_1, \dots, a_k \rangle$. Write

$$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \dots & a_k & 1 \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^k(a_1) & \sigma^k(a_2) & \dots & \sigma^k(a_k) & \sigma^k \end{vmatrix}.$$

Minimum polynomials (continued)

Note Composition of K-endomorphisms of L corresponds to the following *skew* multiplication of polynomials in σ

$$\left(\sum a_i \sigma^i\right) \circ \left(\sum b_j \sigma^j\right) = \sum a_i b_j^{\sigma^i} \sigma^{i+j}$$

Lemma

Suppose $U \subseteq \ker p(\sigma)$ *for some subspace* U *of* L *of dimension* k*. Then*

$$p(\sigma) = q(\sigma) \circ m_U(\sigma).$$

Corollary

All polynomials of degree k *that annihilate* U *are left* $L^\times$*-multiples of each other.*

We refer to these as minimum polynomials for U.

Special Case : hyperplanes

Suppose $U = \langle a_1, \dots, a_{n-1} \rangle = a^{-1}T$ is a K-hyperplane in L. So $a = \langle a_1, \dots, a_{n-1} \rangle^\perp$.

Two minimum polynomials for U :

- $$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & 1 \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_{n-1}) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \dots & \sigma^{n-1}(a_{n-1}) & \sigma^{n-1} \end{vmatrix}.$$
- $m'_U(\sigma) = a^{\sigma^{n-1}}\sigma^{n-1} + a^{\sigma^{n-2}}\sigma^{n-2} + \dots + a^\sigma\sigma + a$

These two polynomials must be $L^\times$-multiples of each other.

If n is odd, it follows that a is a $K^\times$-multiple of the constant term of $m_U(\sigma)$. Thus in this case

$$\langle a_1, \dots, a_{n-1} \rangle^\perp = \langle |\sigma^i(a_j)| \rangle_{1 \leq i, j \leq n-1}.$$

Special Case : hyperplanes

Suppose $U = \langle a_1, \ldots, a_{n-1} \rangle = a^{-1}T$ is a K-hyperplane in L.
So $a = \langle a_1, \ldots, a_{n-1} \rangle^{\perp}$.
Two minimum polynomials for U :

- $$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \ldots & a_{n-1} & 1 \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_{n-1}) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \ldots & \sigma^{n-1}(a_{n-1}) & \sigma^{n-1} \end{vmatrix}.$$
- $m'_U(\sigma) = a^{\sigma^{n-1}}\sigma^{n-1} + a^{\sigma^{n-2}}\sigma^{n-2} + \cdots + a^{\sigma}\sigma + a$

These two polynomials must be $L^{\times}$-multiples of each other.

If n is odd, it follows that a is a $K^{\times}$-multiple of the constant term of $m_U(\sigma)$. Thus in this case

$$\langle a_1, \ldots, a_{n-1} \rangle^{\perp} = \left\langle \left| \sigma^i(a_j) \right| \right\rangle_{1 \leq i, j \leq n-1}.$$

Special Case : hyperplanes

Suppose $U = \langle a_1, \ldots, a_{n-1} \rangle = a^{-1}T$ is a K-hyperplane in L.
So $a = \langle a_1, \ldots, a_{n-1} \rangle^{\perp}$.
Two minimum polynomials for U :

- $$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \ldots & a_{n-1} & 1 \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_{n-1}) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \ldots & \sigma^{n-1}(a_{n-1}) & \sigma^{n-1} \end{vmatrix}.$$
- $m'_U(\sigma) = a^{\sigma^{n-1}}\sigma^{n-1} + a^{\sigma^{n-2}}\sigma^{n-2} + \cdots + a^{\sigma}\sigma + a$

These two polynomials must be $L^{\times}$-multiples of each other.

If n is odd, it follows that a is a $K^{\times}$-multiple of the constant term of $m_U(\sigma)$. Thus in this case

$$\langle a_1, \ldots, a_{n-1} \rangle^{\perp} = \left\langle \left| \sigma^i(a_j) \right| \right\rangle_{1 \le i, j \le n-1}.$$

Special Case : hyperplanes

Suppose $U = \langle a_1, \ldots, a_{n-1} \rangle = a^{-1} T$ is a K-hyperplane in L.
So $a = \langle a_1, \ldots, a_{n-1} \rangle^{\perp}$.
Two minimum polynomials for U :

- $$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \ldots & a_{n-1} & 1 \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_{n-1}) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \ldots & \sigma^{n-1}(a_{n-1}) & \sigma^{n-1} \end{vmatrix}.$$
- $m'_U(\sigma) = a^{\sigma^{n-1}} \sigma^{n-1} + a^{\sigma^{n-2}} \sigma^{n-2} + \cdots + a^{\sigma} \sigma + a$

These two polynomials must be $L^{\times}$-multiples of each other.

If n is odd, it follows that a is a $K^{\times}$-multiple of the constant term of $m_U(\sigma)$. Thus in this case

$$\langle a_1, \ldots, a_{n-1} \rangle^{\perp} = \langle \left| \sigma^i(a_j) \right| \rangle_{1 \leq i, j \leq n-1}.$$

Special Case : hyperplanes

Suppose $U = \langle a_1, \ldots, a_{n-1} \rangle = a^{-1}T$ is a K-hyperplane in L.
So $a = \langle a_1, \ldots, a_{n-1} \rangle^{\perp}$.
Two minimum polynomials for U :

- $$m_U(\sigma) = \begin{vmatrix} a_1 & a_2 & \ldots & a_{n-1} & 1 \\ \sigma(a_1) & \sigma(a_2) & \ldots & \sigma(a_{n-1}) & \sigma \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \ldots & \sigma^{n-1}(a_{n-1}) & \sigma^{n-1} \end{vmatrix}.$$
- $m'_U(\sigma) = a^{\sigma^{n-1}}\sigma^{n-1} + a^{\sigma^{n-2}}\sigma^{n-2} + \cdots + a^{\sigma}\sigma + a$

These two polynomials must be $L^{\times}$-multiples of each other.

If n is odd, it follows that a is a $K^{\times}$-multiple of the constant term of $m_U(\sigma)$. Thus in this case

$$\langle a_1, \ldots, a_{n-1} \rangle^{\perp} = \left\langle \left| \sigma^i(a_j) \right| \right\rangle_{1 \leq i, j \leq n-1}.$$

Further properties for odd degree extensions

Suppose that n is odd and let $U = \langle a_1, \ldots, a_k \rangle$ be a subspace of L of dimension $k < n-1$. Then

$$U^\perp = \left\{ \begin{vmatrix} a_1^\sigma & \ldots & a_k^\sigma & x_{k+1}^\sigma & \ldots & x_{n-1}^\sigma \\ a_1^{\sigma^2} & \ldots & a_k^{\sigma^2} & x_{k+1}^{\sigma^2} & \ldots & x_{n-1}^{\sigma^2} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_1^{\sigma^{n-1}} & \ldots & a_k^{\sigma^{n-1}} & x_{k+1}^{\sigma^{n-1}} & \ldots & x_{n-1}^{\sigma^{n-1}} \end{vmatrix} \right\}_{x_j \in L}$$

Note If $k = n-2$, this is saying that the image of a minimum polynomial for U is a $L^\times$-translate of $\sigma^{-1}(U^\perp)$.

Another Construction

Let $U = \langle a_1, \dots, a_k \rangle$ be a subspace of L of dimension k. A minimum polynomial for the orthogonal complement $U^\perp$ of U is given by

$$m_{U^\perp}(\sigma) = \sum_{i=0}^{n-k} \begin{vmatrix} \sigma^i(a_1) & \dots & \sigma^i(a_k) \\ \sigma^{n-k+1}(a_1) & \dots & \sigma^{n-k+1}(a_k) \\ \sigma^{n-k+2}(a_1) & \dots & \sigma^{n-k+2}(a_k) \\ \vdots & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \dots & \sigma^{n-1}(a_k) \end{vmatrix} \sigma^i.$$

If $x \in L$, then

$$m_{U^\perp}(x) = \sigma^{n-k} \left(\begin{vmatrix} \mathrm{Tr}(a_1 x) & \mathrm{Tr}(a_2 x) & \dots & \mathrm{Tr}(a_k x) \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \\ \sigma^2(a_1) & \sigma^2(a_2) & \dots & \sigma^2(a_k) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-1}(a_1) & \sigma^{k-1}(a_2) & \dots & \sigma^{k-1}(a_k) \end{vmatrix} \right)$$

Another Construction

Let $U = \langle a_1, \dots, a_k \rangle$ be a subspace of L of dimension k. A minimum polynomial for the orthogonal complement $U^\perp$ of U is given by

$$m_{U^\perp}(\sigma) = \sum_{i=0}^{n-k} \begin{vmatrix} \sigma^i(a_1) & \dots & \sigma^i(a_k) \\ \sigma^{n-k+1}(a_1) & \dots & \sigma^{n-k+1}(a_k) \\ \sigma^{n-k+2}(a_1) & \dots & \sigma^{n-k+2}(a_k) \\ \vdots & \vdots & \vdots \\ \sigma^{n-1}(a_1) & \dots & \sigma^{n-1}(a_k) \end{vmatrix} \sigma^i.$$

If $x \in L$, then

$$m_{U^\perp}(x) = \sigma^{n-k} \left(\begin{vmatrix} \mathrm{Tr}(a_1 x) & \mathrm{Tr}(a_2 x) & \dots & \mathrm{Tr}(a_k x) \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \\ \sigma^2(a_1) & \sigma^2(a_2) & \dots & \sigma^2(a_k) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-1}(a_1) & \sigma^{k-1}(a_2) & \dots & \sigma^{k-1}(a_k) \end{vmatrix} \right)$$

Last slide before conference dinner

Note $U \sim V$ means that the subspaces U and V of L are $L^{\times}$-translates of each other.

If $U = \langle a_1, \ldots, a_k \rangle$, write A for the $k \times k$ matrix whose (i, j) entry is $\sigma^{i-1}(a_j)$. Let m_i denote the minor of the entry in the $(1, i)$-position of A, and let U^* denote the space generated by the m_i.

Let m_U and $m_{U^\perp}$ be minimum polynomials for U and $U^\perp$. Then

1. $m_U(L) \sim (U^*)^\perp$
2. $m_{U^\perp}(L) \sim \sigma^{n-k}(U^*)$
3. $U^{**} \sim \sigma^k(U)$
4. $U^\perp$ is a $L^\times$-translate of the image of a minimum polynomial for the space $\sigma^{-k}(U^*)$