Minimum polynomials and spaces of matrices with special rank properties

joint work with R. Gow

Rachel Quinlan

June 21, 2010

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

Plan

The Setup

Rank

Spaces of skew-symmetric matrices

Fields admitting cyclic extensions

- Let K be a field that admits a cyclic Galois extension L of degree n.
- Let σ be a generator of the Galois group $\mathrm{Gal}(L/K)$. Any vector space V of dimension n over K is isomorphic (as a vector space) to L
- Every K-linear transformation of V corresponds to a K-linear transformation of L; these can be described in terms of σ.

Linear Independence of Characters

Any expression of the form

$$\sum_{i=0}^{n-1} a_i\sigma^i, \quad a_i \in L$$

may be interpreted as a K-linear endomorphism of L, according to

$$\left(\sum_{i=0}^{n-1} a_i\sigma^i\right)(x) = \sum_{i=1}^{n-1} a_i\sigma^i(x), \text{ for } x \in L.$$

Theorem (Artin : Independence of Characters)

Every K-linear endomorphism of L has a unique expression as a "L-polynomial" in σ of degree at most $n-1$.

We use this idea to define the *degree* of an element of $\mathrm{End}_K(L)$.

A Determinant

Lemma

Let $a_1, a_2, \ldots, a_k$ be non–zero elements of L. Then

$$\det \begin{pmatrix} a_1 & a_1^{\sigma} & \ldots & a_1^{\sigma^{k-1}} \\ a_2 & a_2^{\sigma} & \ldots & a_2^{\sigma^{k-1}} \\ \vdots & \vdots & \ldots & \vdots \\ a_k & a_k^{\sigma} & \ldots & a_k^{\sigma^{k-1}} \end{pmatrix} \neq 0$$

if and only if $\{a_1, a_2, \ldots, a_k\}$ is linearly independent over K.

Write $b_i = a_i(a_1)^{-1}$. Then

A Determinant

Lemma

Let $a_1, a_2, \ldots, a_k$ be non–zero elements of L. Then

$$\det \begin{pmatrix} a_1 & a_1^{\sigma} & \ldots & a_1^{\sigma^{k-1}} \\ a_2 & a_2^{\sigma} & \ldots & a_2^{\sigma^{k-1}} \\ \vdots & \vdots & \ldots & \vdots \\ a_k & a_k^{\sigma} & \ldots & a_k^{\sigma^{k-1}} \end{pmatrix} \neq 0$$

if and only if $\{a_1, a_2, \ldots, a_k\}$ is linearly independent over K.

Write $b_i = a_i(a_1)^{-1}$. Then

A Determinant

Lemma

Let $a_1, a_2, \ldots, a_k$ be non–zero elements of L. Then

$$\det \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ b_2 & b_2^\sigma - b_2 & (b_2^\sigma - b_2)^\sigma & \ldots & (b_2^\sigma - b_2)^{\sigma^{k-2}} \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ b_k & b_k^\sigma - b_2 & (b_k^\sigma - b_k)^\sigma & \ldots & (b_k^\sigma - b_k)^{\sigma^{k-2}} \end{pmatrix} \neq 0$$

if and only if $\{a_1, a_2, \ldots, a_k\}$ is linearly independent over K.

Write $b_i = a_i(a_1)^{-1}$. Then

The rank of an endomorphism

Theorem

Let $\theta \in \mathrm{End}_K(L)$ *have degree* k*. Write*

$$\theta = b_k\sigma^k + b_{k-1}\sigma^{k-1} + \cdots + b_1\sigma + b_0 id.$$

Then $\dim\ker\theta \leq k$*.*

If $\{a_1, \ldots, a_{k+1}\} \subset \ker\theta$ then

$$\begin{pmatrix} a_1 & a_1^{\sigma} & \ldots & a_1^{\sigma^k} \\ a_2 & a_2^{\sigma} & \ldots & a_2^{\sigma^k} \\ \vdots & \vdots & \ldots & \vdots \\ a_{k+1} & a_{k+1}^{\sigma} & \ldots & a_{k+1}^{\sigma^k} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The rank of an endomorphism

Theorem

Let $\theta \in \mathrm{End}_K(L)$ *have degree* k. *Write*

$$\theta = b_k\sigma^k + b_{k-1}\sigma^{k-1} + \cdots + b_1\sigma + b_0 id.$$

Then $\dim\ker\theta \leq k$.

If $\{a_1, \ldots, a_{k+1}\} \subset \ker\theta$ then

$$\begin{pmatrix} a_1 & a_1^{\sigma} & \ldots & a_1^{\sigma^k} \\ a_2 & a_2^{\sigma} & \ldots & a_2^{\sigma^k} \\ \vdots & \vdots & \ldots & \vdots \\ a_{k+1} & a_{k+1}^{\sigma} & \ldots & a_{k+1}^{\sigma^k} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Subspaces of invertible elements

For $i = 0, \ldots, n-1$ define

$$A_i = L\sigma^i = \{a\sigma^i : a \in L\}.$$

Then A_i is a subspace of $\mathrm{End}_K(L)$ of dimension n and all of its non-zero elements are invertible.
Moreover

$$\mathrm{End}_K(L) = \bigoplus_{i=0}^{n-1} A_i,$$

and for $k = 0, \ldots, n-1$ every non-zero element of

$$\bigoplus_{i=0}^{k} A_i$$

has rank at least $n-k$.

A Matrix Version

Corollary

Let K be a field that admits a cyclic Galois extension of degree n. Then $M_n(K)$ contains subspaces $A_1, \ldots, A_n$ with the following properties

- *Each A_i has dimension n*
- *Every non–zero element of each A_i is invertible*
- $M_n(K) = A_1 \oplus A_2 \oplus \cdots \oplus A_n$
- *Every non-zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - k + 1$.*

A Matrix Version

Corollary

Let K be a field that admits a cyclic Galois extension of degree n. Then $M_n(K)$ contains subspaces $A_1, \ldots, A_n$ with the following properties

- *Each A_i has dimension n*
- *Every non–zero element of each A_i is invertible*
- $M_n(K) = A_1 \oplus A_2 \oplus \cdots \oplus A_n$
- *Every non-zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - k + 1$.*

A Matrix Version

Corollary

Let K be a field that admits a cyclic Galois extension of degree n. Then $M_n(K)$ contains subspaces $A_1, \ldots, A_n$ with the following properties

- *Each A_i has dimension n*
- *Every non–zero element of each A_i is invertible*
- $M_n(K) = A_1 \oplus A_2 \oplus \cdots \oplus A_n$
- *Every non-zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - k + 1$.*

A Matrix Version

Corollary

Let K be a field that admits a cyclic Galois extension of degree n. Then $M_n(K)$ contains subspaces $A_1, \ldots, A_n$ with the following properties

- *Each A_i has dimension n*
- *Every non–zero element of each A_i is invertible*
- $M_n(K) = A_1 \oplus A_2 \oplus \cdots \oplus A_n$
- *Every non-zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - k + 1$.*

Alternating bilinear forms on L

From now on suppose that n is odd.
Write $\hat{L}$ for $\mathrm{Hom}_K(L, K)$.

For $i \in \{1, \ldots, \frac{n-1}{2}\}$ and $f \in \hat{L}$ define an alternating K-bilinear form $\tau_{f,i}$ on L by

$$\tau_{f,i}(x, y) = f(x^{\sigma^i} y - xy^{\sigma^i}).$$

Then

$$\mathrm{rad}(\tau_{f,i}) = \{a \in L : a^{\sigma^i} y - ay^{\sigma^i} \in \ker f \ \forall y \in L\}$$

is a space of dimension 1 over the fixed field of σ^i in L.

Alternating bilinear forms on L

From now on suppose that n is odd.
Write $\hat{L}$ for $\mathrm{Hom}_K(L, K)$.

For $i \in \{1, \ldots, \frac{n-1}{2}\}$ and $f \in \hat{L}$ define an alternating K-bilinear form $\tau_{f,i}$ on L by

$$\tau_{f,i}(x, y) = f(x^{\sigma^i} y - x y^{\sigma^i}).$$

Then

$$\mathrm{rad}(\tau_{f,i}) = \{a \in L : a^{\sigma^i} y - a y^{\sigma^i} \in \ker f \ \forall y \in L\}$$

is a space of dimension 1 over the fixed field of σ^i in L.

Constant rank spaces of alternating forms

So

$$A_i := \{\tau_{f,i}\}$$

is a space of dimension n of alternating bilinear forms in which every non–zero element has rank $n - \gcd(n, i)$.
Let $\mathrm{Alt}_K(L)$ denote the full space of alternating K-bilinear forms on L; it has dimension $n\left(\frac{n-1}{2}\right)$.

Theorem

1. $\mathrm{Alt}_K(L) = A_1 \oplus A_2 \oplus \cdots \oplus A_{\frac{n-1}{2}}$
2. *For $k = 1, \ldots, \frac{n-1}{2}$, every non–zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - 2k + 1$.*

Note Let $f \in \hat{L}$. Then there exists $b \in L$ for which

$$f(x) = \mathrm{Trace}_{L/K}(bx), \ \forall\, x \in L.$$

Constant rank spaces of alternating forms

So

$$A_i := \{\tau_{f,i}\}$$

is a space of dimension n of alternating bilinear forms in which every non–zero element has rank $n - \gcd(n, i)$.
Let $\mathrm{Alt}_K(L)$ denote the full space of alternating K-bilinear forms on L; it has dimension $n\left(\frac{n-1}{2}\right)$.

Theorem

1. $\mathrm{Alt}_K(L) = A_1 \oplus A_2 \oplus \cdots \oplus A_{\frac{n-1}{2}}$
2. *For $k = 1, \ldots, \frac{n-1}{2}$, every non–zero element of $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ has rank at least $n - 2k + 1$.*

Note Let $f \in \hat{L}$. Then there exists $b \in L$ for which

$$f(x) = \mathrm{Trace}_{L/K}(bx),\ \forall\ x \in L.$$

Constant rank spaces of alternating forms

So

$$A_i := \{\tau_{f,i}\}$$

is a space of dimension n of alternating bilinear forms in which every non–zero element has rank $n - \gcd(n, i)$.
Let $\mathrm{Alt}_K(L)$ denote the full space of alternating K-bilinear forms on L; it has dimension $n\left(\frac{n-1}{2}\right)$.

Theorem

1. $\mathrm{Alt}_K(L) = A_1 \oplus A_2 \oplus \cdots \oplus A_{\frac{n-1}{2}}$
2. *For* $k = 1, \ldots, \frac{n-1}{2}$, *every non–zero element of* $A_1 \oplus A_2 \oplus \cdots \oplus A_k$ *has rank at least* $n - 2k + 1$.

Note Let $f \in \hat{L}$. Then there exists $b \in L$ for which

$$f(x) = \mathrm{Trace}_{L/K}(bx),\ \forall\, x \in L.$$

Proof Outline

For $\theta \in A_1 \oplus \cdots \oplus A_k$ suppose $x \in \operatorname{rad}\theta$. Then

$$\mathrm{Trace}_{\mathrm{L/K}}\left(\sum_{i=1}^{k} b_i(x^{\sigma^i}y - xy^{\sigma^i})\right) = 0,\ \forall y \in L.$$

This means

$$\mathrm{Trace}_{\mathrm{L/K}}\left(\sum b_i x^{\sigma^i} y - \sum b_i x y^{\sigma^i}\right) = 0,\ \forall\ y \in L.$$

Hence $\mathrm{Trace}_{\mathrm{L/K}}\left(\left(\sum b_i x^{\sigma^i} - \sum b_i^{\sigma^{-i}} x^{\sigma^{-i}}\right) y\right) = 0,\ \forall\ y \in L.$

So

$$\sum_{i=1}^{k}\left(-b_i^{\sigma^{k-i}} x^{\sigma^{k-i}} + b_i^{\sigma^k} x^{\sigma^{i+k}}\right) = 0,$$

and x belongs to a space of odd dimension at most equal to $2k$, hence at most $2k-1$.

Proof Outline

For $\theta \in A_1 \oplus \cdots \oplus A_k$ suppose $x \in \operatorname{rad}\theta$. Then

$$\mathrm{Trace}_{L/K}\left(\sum_{i=1}^{k} b_i(x^{\sigma^i}y - xy^{\sigma^i})\right) = 0,\ \forall y \in L.$$

This means

$$\mathrm{Trace}_{L/K}\left(\sum b_i x^{\sigma^i} y - \sum b_i x y^{\sigma^i}\right) = 0,\ \forall\ y \in L.$$

Hence $\mathrm{Trace}_{L/K}\left(\left(\sum b_i x^{\sigma^i} - \sum b_i^{\sigma^{-i}} x^{\sigma^{-i}}\right) y\right) = 0,\ \forall\ y \in L.$

So

$$\sum_{i=1}^{k}\left(-b_i^{\sigma^{k-i}} x^{\sigma^{k-i}} + b_i^{\sigma^k} x^{\sigma^{i+k}}\right) = 0,$$

and x belongs to a space of odd dimension at most equal to $2k$, hence at most $2k-1$.

A Matrix Version

Theorem

Let n be odd, and let K be a field that admits cyclic Galois extensions of degree n. Then the space of skew-symmetric $n \times n$ matrices with entries in K has a direct sum decomposition

$$A_1 \oplus \cdots \oplus A_{\frac{n-1}{2}}$$

where

- *Each A_i has dimension n*
- *Every non–zero element of A_i has rank $n - \gcd(n, i)$*
- *For $k = 1, \ldots, n$, every non–zero element of $A_1 \oplus A_2 \cdots \oplus A_k$ has rank at least $n - 2k + 1$.*

A Matrix Version

Theorem

Let n be odd, and let K be a field that admits cyclic Galois extensions of degree n. Then the space of skew-symmetric $n \times n$ matrices with entries in K has a direct sum decomposition

$$A_1 \oplus \cdots \oplus A_{\frac{n-1}{2}}$$

where

- *Each A_i has dimension n*
- *Every non–zero element of A_i has rank $n - \gcd(n, i)$*
- *For $k = 1, \ldots, n$, every non–zero element of $A_1 \oplus A_2 \cdots \oplus A_k$ has rank at least $n - 2k + 1$.*

A Matrix Version

Theorem

Let n be odd, and let K be a field that admits cyclic Galois extensions of degree n. Then the space of skew-symmetric $n \times n$ matrices with entries in K has a direct sum decomposition

$$A_1 \oplus \cdots \oplus A_{\frac{n-1}{2}}$$

where

- *Each A_i has dimension n*
- *Every non–zero element of A_i has rank $n - \gcd(n, i)$*
- *For $k = 1, \ldots, n$, every non–zero element of $A_1 \oplus A_2 \cdots \oplus A_k$ has rank at least $n - 2k + 1$.*

Grazie e Arrivederci

Forza Azzurri !!!