Galois Invariance, Trace and Subfield Subcodes

Andrea Previtali
(joint with M. Giorgetti)

Department of Physics and Mathematics
University of Insubria-Como, Italy

Ischia, 14-17 April 2010

To Karl and Silvia

Galois Codes

Definitions

- Given a field E and an integer n, a linear code is a subspace L of E^n
- We call n the length of L
- If L has dimension k and minimum distance d, we call L a (n, k, d)-code
- We may consider $n = n(L)$, $k = k(L)$ and $d = d(L)$ as functions of L

Definitions

- Given a field E and an integer n, a linear code is a subspace L of E^n
- We call n the length of L
- If L has dimension k and minimum distance d, we call L a (n, k, d)-code
- We may consider $n = n(L)$, $k = k(L)$ and $d = d(L)$ as functions of L

Definitions

- Given a field E and an integer n, a linear code is a subspace L of E^n
- We call n the length of L
- If L has dimension k and minimum distance d, we call L a (n, k, d)-code
- We may consider $n = n(L)$, $k = k(L)$ and $d = d(L)$ as functions of L

Definitions

- Given a field E and an integer n, a linear code is a subspace L of E^n
- We call n the length of L
- If L has dimension k and minimum distance d, we call L a (n, k, d)-code
- We may consider $n = n(L)$, $k = k(L)$ and $d = d(L)$ as functions of L

Restriction Functor

- Assume K subfield of E
- Consider $C = L \cap K^n$, C is a K-linear code of length n
- What about $k(C)$ and $d(C)$?
- We would like to study the restriction map

$$Res : L \mapsto L \cap K^n$$

from the category of E-linear to the category of K-linear codes

Restriction Functor

- Assume K subfield of E
- Consider $C = L \cap K^n$, C is a K-linear code of length n
- What about $k(C)$ and $d(C)$?
- We would like to study the restriction map

$$Res : L \mapsto L \cap K^n$$

from the category of E-linear to the category of K-linear codes

Restriction Functor

- Assume K subfield of E
- Consider $C = L \cap K^n$, C is a K-linear code of length n
- What about $k(C)$ and $d(C)$?
- We would like to study the restriction map

$$Res : L \mapsto L \cap K^n$$

from the category of E-linear to the category of K-linear codes

Restriction Functor

- Assume K subfield of E
- Consider $C = L \cap K^n$, C is a K-linear code of length n
- What about $k(C)$ and $d(C)$?
- We would like to study the restriction map

$$Res : L \mapsto L \cap K^n$$

from the category of E-linear to the category of K-linear codes

- Let $G = Gal(E/K) = C_{Aut(E)}(K)$
- Any $\gamma \in G$ extends to a K-linear map of E^n via

$$(x_1, \ldots, x_n)^\gamma := (x_1^\gamma, \ldots, x_n^\gamma).$$

- Then $Res(L) = Res(L^\gamma)$, but in general $L \neq L^\gamma$

- Let $G = Gal(E/K) = C_{Aut(E)}(K)$
- Any $\gamma \in G$ extends to a K-linear map of E^n via

$$(x_1, \ldots, x_n)^\gamma := (x_1^\gamma, \ldots, x_n^\gamma).$$

- Then $Res(L) = Res(L^\gamma)$, but in general $L \neq L^\gamma$

- Let $G = Gal(E/K) = C_{Aut(E)}(K)$
- Any $\gamma \in G$ extends to a K-linear map of E^n via

$$(x_1, \dots, x_n)^\gamma := (x_1^\gamma, \dots, x_n^\gamma).$$

- Then $Res(L) = Res(L^\gamma)$, but in general $L \neq L^\gamma$

Automorphism Invariance

- Define $L_G = \bigcap_{\gamma \in G} L^\gamma$, the G-core of L
- L_G is G-invariant
- L is G-invariant iff $L = L_G$
- $Res(L_G) = Res(L)$
- Res may be injective only on G-invariant codes

Automorphism Invariance

- Define $L_G = \bigcap_{\gamma \in G} L^{\gamma}$, the G-core of L
- L_G is G-invariant
- L is G-invariant iff $L = L_G$
- $Res(L_G) = Res(L)$
- Res may be injective only on G-invariant codes

Automorphism Invariance

- Define $L_G = \bigcap_{\gamma \in G} L^\gamma$, the G-core of L
- L_G is G-invariant
- L is G-invariant iff $L = L_G$
- $Res(L_G) = Res(L)$
- Res may be injective only on G-invariant codes

Automorphism Invariance

- Define $L_G = \bigcap_{\gamma \in G} L^\gamma$, the G-core of L
- L_G is G-invariant
- L is G-invariant iff $L = L_G$
- $Res(L_G) = Res(L)$
- Res may be injective only on G-invariant codes

Automorphism Invariance

- Define $L_G = \bigcap_{\gamma \in G} L^{\gamma}$, the G-core of L
- L_G is G-invariant
- L is G-invariant iff $L = L_G$
- $Res(L_G) = Res(L)$
- Res may be injective only on G-invariant codes

(Counter)Example

- $K = \mathbb{Q}$
- $E = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$
- $G = \{id_E\}$
- $L = E(1, \alpha) \leq E^2$
- Then $L_G = L$ but $Res(L) = 0 = Res(0)$

(Counter)Example

- $K = \mathbb{Q}$
- $E = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$
- $G = \{id_E\}$
- $L = E(1, \alpha) \leq E^2$
- Then $L_G = L$ but $Res(L) = 0 = Res(0)$

(Counter)Example

- $K = \mathbb{Q}$
- $E = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$
- $G = \{id_E\}$
- $L = E(1, \alpha) \leq E^2$
- Then $L_G = L$ but $Res(L) = 0 = Res(0)$

(Counter)Example

- $K = \mathbb{Q}$
- $E = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$
- $G = \{id_E\}$
- $L = E(1, \alpha) \leq E^2$
- Then $L_G = L$ but $Res(L) = 0 = Res(0)$

(Counter)Example

- $K = \mathbb{Q}$
- $E = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$
- $G = \{id_E\}$
- $L = E(1, \alpha) \leq E^2$
- Then $L_G = L$ but $Res(L) = 0 = Res(0)$

Galois Extensions

- Assume E/K is Galois
- Let $G = Gal(E/K)$, then $K = C_E(G)$
- Define $Ext(C) = E \otimes_K C$
- Ext defines a functor from K-linear codes to G-invariant E-linear codes

Galois Extensions

- Assume E/K is Galois
- Let $G = Gal(E/K)$, then $K = C_E(G)$
- Define $Ext(C) = E \otimes_K C$
- Ext defines a functor from K-linear codes to G-invariant E-linear codes

Galois Extensions

- Assume E/K is Galois
- Let $G = Gal(E/K)$, then $K = C_E(G)$
- Define $Ext(C) = E \otimes_K C$
- Ext defines a functor from K-linear codes to G-invariant E-linear codes

Galois Extensions

- Assume E/K is Galois
- Let $G = Gal(E/K)$, then $K = C_E(G)$
- Define $Ext(C) = E \otimes_K C$
- *Ext* defines a functor from K-linear codes to G-invariant E-linear codes

Ext vs Res

-

Theorem

E/K Galois, $G = Gal(E/K)$, $L \leq E^n$. Then L is G-invariant iff $L = Ext(Res(L))$ iff L admits a basis in K^n.

- Obviously $Ext(Res(L))$ is G-invariant
- $L = L_G$, b Gauss-Jordan reduced normalized basis

$$b_i = (0, \dots, 0, 1, \dots)$$

lie in K^n

Ext vs Res

- **Theorem**

  E/K Galois, $G = Gal(E/K)$, $L \leq E^n$. Then L is G-invariant iff $L = Ext(Res(L))$ iff L admits a basis in K^n.

  - Obviously $Ext(Res(L))$ is G-invariant
  - $L = L_G$, b Gauss-Jordan reduced normalized basis

$$b_i = (0, \dots, 0, 1, \dots)$$

lie in K^n

Ext vs Res

- **Theorem**

  E/K Galois, $G = Gal(E/K)$, $L \leq E^n$. Then L is G-invariant iff $L = Ext(Res(L))$ iff L admits a basis in K^n.

  - Obviously $Ext(Res(L))$ is G-invariant
  - $L = L_G$, b Gauss-Jordan reduced normalized basis

    $$b_i = (0, \dots, 0, 1, \dots)$$

    lie in K^n

Ext vs Res

- **Theorem**

  E/K Galois, $G = Gal(E/K)$, $L \leq E^n$. Then L is G-invariant iff $L = Ext(Res(L))$ iff L admits a basis in K^n.

  - Obviously $Ext(Res(L))$ is G-invariant
  - $L = L_G$, b Gauss-Jordan reduced normalized basis

    $$b_i = (0, \dots, 0, 1, \dots)$$

    lie in K^n

Ext vs Res

-

Corollary

$L_G = Ext(Res(L))$

- *Ext* and *Res* are inverse maps from the category of G-invariant E-linear codes and K-linear codes
- Different proof using cohomology tools
- Cohomology is just sophisticated linear algebra

Ext vs Res

- **Corollary**

  $L_G = Ext(Res(L))$

  - *Ext* and *Res* are inverse maps from the category of G-invariant E-linear codes and K-linear codes
  - Different proof using cohomology tools
  - Cohomology is just sophisticated linear algebra

Ext vs Res

- **Corollary**

  $L_G = Ext(Res(L))$

  - *Ext* and *Res* are inverse maps from the category of *G*-invariant *E*-linear codes and *K*-linear codes
  - Different proof using cohomology tools
  - Cohomology is just sophisticated linear algebra

Ext vs Res

- **Corollary**

  $L_G = Ext(Res(L))$

  - *Ext* and *Res* are inverse maps from the category of G-invariant E-linear codes and K-linear codes
  - Different proof using cohomology tools
  - Cohomology is just sophisticated linear algebra

Ext vs Res

- **Corollary**

  $L_G = Ext(Res(L))$

  - *Ext* and *Res* are inverse maps from the category of G-invariant E-linear codes and K-linear codes
  - Different proof using cohomology tools
  - Cohomology is just sophisticated linear algebra

Trace Codes

- E/K Galois, Tr the Trace map extends to E^n

$$\mathrm{Tr}((c_1,\ldots,c_n)) = (\mathrm{Tr}(c_1),\ldots,\mathrm{Tr}(c_n))$$

- Define $\mathrm{Tr}(L) = \{\mathrm{Tr}(c) : c \in L\} \leq K^n$
- Dual code $L^\perp = \{v \in E^n : L \cdot v^t = 0\}$
-

Theorem (Delsarte, 1975)

Let E/K Galois, L a E-linear code, then

$$Res(L)^\perp = \mathrm{Tr}(L^\perp)$$

Trace Codes

- E/K Galois, Tr the Trace map extends to E^n

$$\mathrm{Tr}((c_1, \ldots, c_n)) = (\mathrm{Tr}(c_1), \ldots, \mathrm{Tr}(c_n))$$

- Define $\mathrm{Tr}(L) = \{\mathrm{Tr}(c) \,:\, c \in L\} \leq K^n$
- Dual code $L^\perp = \{v \in E^n \,:\, L \cdot v^t = 0\}$
-

Theorem (Delsarte, 1975)

Let E/K Galois, L a E-linear code, then

$$Res(L)^\perp = \mathrm{Tr}(L^\perp)$$

Trace Codes

- E/K Galois, Tr the Trace map extends to E^n

$$\mathrm{Tr}((c_1,\dots,c_n)) = (\mathrm{Tr}(c_1),\dots,\mathrm{Tr}(c_n))$$

- Define $\mathrm{Tr}(L) = \{\mathrm{Tr}(c) : c \in L\} \leq K^n$
- Dual code $L^\perp = \{v \in E^n : L \cdot v^t = 0\}$
-

Theorem (Delsarte, 1975)

Let E/K Galois, L a E-linear code, then

$$Res(L)^\perp = \mathrm{Tr}(L^\perp)$$

Trace Codes

- E/K Galois, Tr the Trace map extends to E^n

$$\mathrm{Tr}((c_1, \dots, c_n)) = (\mathrm{Tr}(c_1), \dots, \mathrm{Tr}(c_n))$$

- Define $\mathrm{Tr}(L) = \{\mathrm{Tr}(c) : c \in L\} \leq K^n$
- Dual code $L^\perp = \{v \in E^n : L \cdot v^t = 0\}$
-

Theorem (Delsarte, 1975)

Let E/K Galois, L a E-linear code, then

$$Res(L)^\perp = \mathrm{Tr}(L^\perp)$$

Trace Codes

- E/K Galois, Tr the Trace map extends to E^n

$$\mathrm{Tr}((c_1,\ldots,c_n)) = (\mathrm{Tr}(c_1),\ldots,\mathrm{Tr}(c_n))$$

- Define $\mathrm{Tr}(L) = \{\mathrm{Tr}(c) \,:\, c \in L\} \leq K^n$
- Dual code $L^\perp = \{v \in E^n \,:\, L \cdot v^t = 0\}$
- **Theorem (Delsarte, 1975)**

  Let E/K Galois, L a E-linear code, then

$$Res(L)^\perp = \mathrm{Tr}(L^\perp)$$

Trace and Restriction

- Both $Res(L)$ and $\text{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\text{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

Trace and Restriction

- Both $Res(L)$ and $\mathrm{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\mathrm{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

Trace and Restriction

- Both $Res(L)$ and $\mathrm{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\mathrm{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

Trace and Restriction

- Both $Res(L)$ and $\mathrm{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\mathrm{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

Trace and Restriction

- Both $Res(L)$ and $\mathrm{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\mathrm{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

Trace and Restriction

- Both $Res(L)$ and $\mathrm{Tr}(L)$ are K-linear codes
- How are they related?
- Let $K = \mathbb{F}_p(x)$, $E = K(\alpha)$, where $\alpha^p = x$
- Then E/K is an inseparable extension
- $\mathrm{Tr}(L) = 0$ for any E-linear code
- But $Res(E^n) = K^n \neq 0$

- Let $|E : K| = 2$, a quadratic extension with char $K \neq 2$
- $E = K[\alpha]$, $\alpha^2 = a \in K$ and $L = Ev$, $v = (1, \alpha)$
- Then $\mathrm{Tr}(v) = (2, 0)$ and $\mathrm{Tr}(\alpha v) = (0, 2a)$
- Thus $\mathrm{Tr}(C) = K^2$ while $Res(C) = 0$

- Let $|E : K| = 2$, a quadratic extension with char $K \neq 2$
- $E = K[\alpha]$, $\alpha^2 = a \in K$ and $L = Ev$, $v = (1, \alpha)$
- Then $\mathrm{Tr}(v) = (2, 0)$ and $\mathrm{Tr}(\alpha v) = (0, 2a)$
- Thus $\mathrm{Tr}(C) = K^2$ while $Res(C) = 0$

- Let $|E:K| = 2$, a quadratic extension with char $K \neq 2$
- $E = K[\alpha]$, $\alpha^2 = a \in K$ and $L = Ev$, $v = (1, \alpha)$
- Then $\mathrm{Tr}(v) = (2, 0)$ and $\mathrm{Tr}(\alpha v) = (0, 2a)$
- Thus $\mathrm{Tr}(C) = K^2$ while $Res(C) = 0$

- Let $|E : K| = 2$, a quadratic extension with char $K \neq 2$
- $E = K[\alpha]$, $\alpha^2 = a \in K$ and $L = Ev$, $v = (1, \alpha)$
- Then $\mathrm{Tr}(v) = (2, 0)$ and $\mathrm{Tr}(\alpha v) = (0, 2a)$
- Thus $\mathrm{Tr}(C) = K^2$ while $Res(C) = 0$

Separable Extensions

- E/K separable, $L \leq E^n$. Then
$$Res(C) \leq \mathrm{Tr}(C)$$
- For $v \in K^n$, $\lambda \in E$,
$$\mathrm{Tr}(\lambda v) = \mathrm{Tr}(\lambda) v.$$
- $\alpha \in E$ such that $\mathrm{Tr}(\alpha) = 1$
- Take $v \in Res(C) = C \cap K^n$, then $v = \mathrm{Tr}(\alpha v) \in \mathrm{Tr}(C)$

Separable Extensions

- E/K separable, $L \leq E^n$. Then

$$Res(C) \leq \mathrm{Tr}(C)$$

- For $v \in K^n$, $\lambda \in E$,

$$\mathrm{Tr}(\lambda v) = \mathrm{Tr}(\lambda) v.$$

- $\alpha \in E$ such that $\mathrm{Tr}(\alpha) = 1$
- Take $v \in Res(C) = C \cap K^n$, then $v = \mathrm{Tr}(\alpha v) \in \mathrm{Tr}(C)$

Separable Extensions

- E/K separable, $L \leq E^n$. Then
$$Res(C) \leq \mathrm{Tr}(C)$$
- For $v \in K^n$, $\lambda \in E$,
$$\mathrm{Tr}(\lambda v) = \mathrm{Tr}(\lambda) v.$$
- $\alpha \in E$ such that $\mathrm{Tr}(\alpha) = 1$
- Take $v \in Res(C) = C \cap K^n$, then $v = \mathrm{Tr}(\alpha v) \in \mathrm{Tr}(C)$

Separable Extensions

- E/K separable, $L \leq E^n$. Then
$$Res(C) \leq \mathrm{Tr}(C)$$
- For $v \in K^n$, $\lambda \in E$,
$$\mathrm{Tr}(\lambda v) = \mathrm{Tr}(\lambda)v.$$
- $\alpha \in E$ such that $\mathrm{Tr}(\alpha) = 1$
- Take $v \in Res(C) = C \cap K^n$, then $v = \mathrm{Tr}(\alpha v) \in \mathrm{Tr}(C)$

- E/K Galois, $G = Gal(E/K)$, $L = L_G \leq E^n$, then

$$Res(L) = \mathrm{Tr}(L)$$

- $\mathrm{Tr}(c) = \sum_{\gamma \in G} c^\gamma \in L$
- $\mathrm{Tr}(c) \in K^n$, then $\mathrm{Tr}(c) \in Res(L)$
- Does the converse hold?

- E/K Galois, $G = Gal(E/K)$, $L = L_G \leq E^n$, then

$$Res(L) = \mathrm{Tr}(L)$$

- $\mathrm{Tr}(c) = \sum_{\gamma \in G} c^\gamma \in L$
- $\mathrm{Tr}(c) \in K^n$, then $\mathrm{Tr}(c) \in Res(L)$
- Does the converse hold?

- E/K Galois, $G = Gal(E/K)$, $L = L_G \leq E^n$, then

$$Res(L) = \mathrm{Tr}(L)$$

- $\mathrm{Tr}(c) = \sum_{\gamma \in G} c^\gamma \in L$
- $\mathrm{Tr}(c) \in K^n$, then $\mathrm{Tr}(c) \in Res(L)$
- Does the converse hold?

- E/K Galois, $G = Gal(E/K)$, $L = L_G \leq E^n$, then

$$Res(L) = \mathrm{Tr}(L)$$

- $\mathrm{Tr}(c) = \sum_{\gamma \in G} c^\gamma \in L$
- $\mathrm{Tr}(c) \in K^n$, then $\mathrm{Tr}(c) \in Res(L)$
- Does the converse hold?

- For any $v \in E^n$, $v \in Ext(\mathrm{Tr}(Ev))$
- $B(\lambda, \mu) := \mathrm{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_m$ trace-dual K-bases of E

$$\mathrm{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \ldots, a_n)$, $a_i = \sum_j a_{ij}\lambda_j$
- Then $\sum_k \lambda_k \mathrm{Tr}(\mu_k a_i) = \sum_k a_{ik}\lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in Ext(\mathrm{Tr}(Ev))$

- For any $v \in E^n$, $v \in Ext(\mathrm{Tr}(Ev))$
- $B(\lambda, \mu) := \mathrm{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_m$ trace-dual K-bases of E

$$\mathrm{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \ldots, a_n)$, $a_i = \sum_j a_{ij}\lambda_j$
- Then $\sum_k \lambda_k \mathrm{Tr}(\mu_k a_i) = \sum_k a_{ik}\lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in Ext(\mathrm{Tr}(Ev))$

- For any $v \in E^n$, $v \in Ext(\mathrm{Tr}(Ev))$
- $B(\lambda, \mu) := \mathrm{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \dots, \lambda_m$ and $\mu_1, \dots, \mu_m$ trace-dual K-bases of E

$$\mathrm{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \dots, a_n)$, $a_i = \sum_j a_{ij}\lambda_j$
- Then $\sum_k \lambda_k \mathrm{Tr}(\mu_k a_i) = \sum_k a_{ik}\lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in Ext(\mathrm{Tr}(Ev))$

- For any $v \in E^n$, $v \in Ext(\text{Tr}(Ev))$
- $B(\lambda, \mu) := \text{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_m$ trace-dual K-bases of E

$$\text{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \ldots, a_n)$, $a_i = \sum_j a_{ij}\lambda_j$
- Then $\sum_k \lambda_k \text{Tr}(\mu_k a_i) = \sum_k a_{ik}\lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \text{Tr}(\mu_k v) \in Ext(\text{Tr}(Ev))$

- For any $v \in E^n$, $v \in Ext(\mathrm{Tr}(Ev))$
- $B(\lambda, \mu) := \mathrm{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \dots, \lambda_m$ and $\mu_1, \dots, \mu_m$ trace-dual K-bases of E

$$\mathrm{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \dots, a_n)$, $a_i = \sum_j a_{ij}\lambda_j$
- Then $\sum_k \lambda_k \mathrm{Tr}(\mu_k a_i) = \sum_k a_{ik}\lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in Ext(\mathrm{Tr}(Ev))$

- For any $v \in E^n$, $v \in Ext(\mathrm{Tr}(Ev))$
- $B(\lambda, \mu) := \mathrm{Tr}(\lambda\mu)$ defines a non-degenerate bilinear K-form on E
- Let $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_m$ trace-dual K-bases of E

$$\mathrm{Tr}(\mu_k \lambda_j) = \delta_{kj}$$

- Let $v = (a_1, \ldots, a_n)$, $a_i = \sum_j a_{ij} \lambda_j$
- Then $\sum_k \lambda_k \mathrm{Tr}(\mu_k a_i) = \sum_k a_{ik} \lambda_k = a_i$
- Thus $v = \sum_k \lambda_k \mathrm{Tr}(\mu_k v) \in Ext(\mathrm{Tr}(Ev))$

•

Theorem

E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

- We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
- L is a counterexample of minimum dimension
- Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
- Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
- So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
- But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

Theorem

E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

- We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
- L is a counterexample of minimum dimension
- Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
- Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
- So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
- But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$

- **Theorem**

  E/K Galois, L a E-linear code. Then $Res(L) = \mathrm{Tr}(L)$ iff $L = L_G$ is Galois invariant

  - We claim $Res(L) = \mathrm{Tr}(L)$ forces $L = L_G$
  - L is a counterexample of minimum dimension
  - Then $\dim(L/L_G) = 1$ and $L = L_G \oplus Ev$
  - Now $\mathrm{Tr}(L_G) = \mathrm{Tr}(L) = \mathrm{Tr}(L_G) + \mathrm{Tr}(Ev)$
  - So $\mathrm{Tr}(Ev) \leq \mathrm{Tr}(L_G)$
  - But $v \in Ext(\mathrm{Tr}(Ev)) \leq Ext(\mathrm{Tr}(L_G)) = L_G$ against $L_G \neq L$