Cohomological invariants of G-Galois algebras

Eva Bayer-Fluckiger

EPFL

June 20, 2017

SELF-DUAL NORMAL BASES

Hendrik LENSTRA (1987) :

Let k be a field, and let K/k be a Galois extension of finite degree. Set $G = \mathrm{Gal}(K/k)$.

SELF-DUAL NORMAL BASES

Hendrik LENSTRA (1987) :

Let k be a field, and let K/k be a Galois extension of finite degree. Set $G = \mathrm{Gal}(K/k)$.

Let $(ge)_{g \in G}$ be a normal basis of K/k, for some $e \in K^\times$. Let

SELF-DUAL NORMAL BASES

Hendrik LENSTRA (1987) :

Let k be a field, and let K/k be a Galois extension of finite degree. Set $G = \mathrm{Gal}(K/k)$.

Let $(ge)_{g \in G}$ be a normal basis of K/k, for some $e \in K^\times$. Let

$$q_K : K \times K \to k$$

$$q_K(x, y) = \mathrm{Tr}_{K/k}(xy)$$

SELF-DUAL NORMAL BASES

Hendrik LENSTRA (1987) :

Let k be a field, and let K/k be a Galois extension of finite degree. Set $G = \mathrm{Gal}(K/k)$.

Let $(ge)_{g \in G}$ be a normal basis of K/k, for some $e \in K^\times$. Let

$$q_K : K \times K \to k$$

$$q_K(x, y) = \mathrm{Tr}_{K/k}(xy)$$

be the trace form of K/k.

SELF-DUAL NORMAL BASES

We say that $(ge)_{g \in G}$ is a self-dual normal basis of K/k if for all $g, h \in G$ we have

SELF-DUAL NORMAL BASES

We say that $(ge)_{g\in G}$ is a self-dual normal basis of K/k if for all $g, h \in G$ we have

$$q_K(ge, ge) = 1$$

and

$$q_K(ge, he) = 0 \text{ if } g \neq h.$$

ABELIAN EXTENSIONS

Theorem. (Lenstra) Assume that G is abelian.

• $\mathrm{char}(k) \neq 2$. Then K/k has a self-dual normal basis $\iff$ the order of G is odd.

ABELIAN EXTENSIONS

Theorem. (Lenstra) Assume that G is abelian.

• $\mathrm{char}(k) \neq 2$. Then K/k has a self-dual normal basis $\iff$ the order of G is odd.

• $\mathrm{char}(k) = 2$. Then K/k has a self-dual normal basis $\iff$ G has no element of order 4.

NON ABELIAN EXTENSIONS

G non abelian ?? In particular,

NON ABELIAN EXTENSIONS

G non abelian ?? In particular,

$$G \text{ has odd order } \implies K/k \text{ has a self-dual normal basis ??}$$

NON ABELIAN EXTENSIONS

G non abelian ?? In particular,

$$G \text{ has odd order } \implies K/k \text{ has a self-dual normal basis ??}$$

Theorem. (E.B - Lenstra, 1990, 1989)

If the order of G is odd, then K/k has a self-dual normal basis.

CHARACTERISTIC 2

Theorem. (Serre, 2014) Assume that $\mathrm{char(k)} = 2$. Then K/k has a self-dual normal basis $\iff$ G is generated by elements of odd order and elements of order 2.

CHARACTERISTIC 2

Theorem. (Serre, 2014) Assume that $\mathrm{char}(\mathrm{k}) = 2$. Then K/k has a self-dual normal basis $\iff$ G is generated by elements of odd order and elements of order 2.

Only depends of the group G , and not of the extension K/k !

EXAMPLE

Example. (E.B. - Serre 1994) $k = \mathbf{Q}$, $G = A_4$. There exist Galois extensions with and without self-dual normal basis.

EXAMPLE

Example. (E.B. - Serre 1994) $k = \mathbf{Q}$, $G = A_4$. There exist Galois extensions with and without self-dual normal basis.

E.B. - Serre 1994 : necessary and sufficient conditions for the existence of a self-dual normal basis when the 2-Sylow subgroups are elementary abelian, or quaternionian of order 8.

EXAMPLE

Example. (E.B. - Serre 1994) $k = \mathbf{Q}$, $G = A_4$. There exist Galois extensions with and without self-dual normal basis.

E.B. - Serre 1994 : necessary and sufficient conditions for the existence of a self-dual normal basis when the 2-Sylow subgroups are elementary abelian, or quaternionian of order 8.

The conditions involve cohomological invariants.

G-GALOIS ALGEBRAS

Assume from now on that $\mathrm{char}(k) \neq 2$. Let G be a finite group.

G-GALOIS ALGEBRAS

Assume from now on that $\mathrm{char}(k) \neq 2$. Let G be a finite group.

Instead of only Galois extensions, consider more generally G-Galois algebras :

G-GALOIS ALGEBRAS

Assume from now on that $\mathrm{char}(k) \neq 2$. Let G be a finite group.

Instead of only Galois extensions, consider more generally G-Galois algebras :

- étale k-algebra L of finite rank,
- with a (left) action of G such that $L \simeq k[G]$.

G-GALOIS ALGEBRAS

Assume from now on that $\mathrm{char}(k) \neq 2$. Let G be a finite group.

Instead of only Galois extensions, consider more generally G-Galois algebras :

- étale k-algebra L of finite rank,
- with a (left) action of G such that $L \simeq k[G]$.

Examples.

- Galois extension with group G;
- Split G-Galois algebra $k \times \cdots \times k$.

G-GALOIS ALGEBRAS

k_s : a separable closure of k, $\Gamma_k = \mathrm{Gal}(k_s/k)$.

G-Galois algebra $\to$ continuous homomorphism $\phi : \Gamma_k \to G$.

G-GALOIS ALGEBRAS

k_s : a separable closure of k, $\Gamma_k = \mathrm{Gal}(k_s/k)$.

G-Galois algebra $\to$ continuous homomorphism $\phi : \Gamma_k \to G$.

Examples.

- ϕ surjective $\iff$ Galois extension;
- $\phi = 1 \iff$ split G-Galois algebra.

G-GALOIS ALGEBRAS

L a G-Galois algebra,

G-GALOIS ALGEBRAS

L a G-Galois algebra,

$$q_L : L \times L \to k$$

$$q_L(x, y) = \mathrm{Tr}_{L/k}(xy)$$

G-GALOIS ALGEBRAS

L a G-Galois algebra,

$$q_L : L \times L \to k$$

$$q_L(x, y) = \mathrm{Tr}_{L/k}(xy)$$

the trace form of L. We say that $(ge)_{g \in G}$ is a self-dual normal basis of L over k if for all $g, h \in G$ we have

$$q_L(ge, ge) = 1$$

and

$$q_L(ge, he) = 0 \text{ if } g \neq h.$$

SELF-DUAL NORMAL BASES

Theorem. (E.B - Lenstra, 1990, 1989)

If the order of G is odd, then every G - Galois algebra has a self-dual normal basis.

SELF-DUAL NORMAL BASES

Theorem. (E.B - Lenstra, 1990, 1989)

If the order of G is odd, then every G - Galois algebra has a self-dual normal basis.

G abelian - Lenstra's result does not hold in general for G-Galois algebras, only for Galois extensions.

SELF-DUAL NORMAL BASES

Theorem. (E.B - Lenstra, 1990, 1989)

If the order of G is odd, then every G - Galois algebra has a self-dual normal basis.

G abelian - Lenstra's result does not hold in general for G-Galois algebras, only for Galois extensions.

Question : Necessary and sufficient condition for the existence of self-dual normal bases.

SELF-DUAL NORMAL BASES

Theorem. (E.B - Lenstra, 1990, 1989)

If the order of G is odd, then every G - Galois algebra has a self-dual normal basis.

G abelian - Lenstra's result does not hold in general for G-Galois algebras, only for Galois extensions.

Question : Necessary and sufficient condition for the existence of self-dual normal bases.

Open even for G abelian.

COHOMOLOGICAL INVARIANTS

Γ a (finite or profinite) group, set $H^n(\Gamma) = H^n(\Gamma, \mathbf{Z}/2\mathbf{Z})$.

COHOMOLOGICAL INVARIANTS

Γ a (finite or profinite) group, set $H^n(\Gamma) = H^n(\Gamma, \mathbf{Z}/2\mathbf{Z})$.

$H^n(k) = H^n(\Gamma_k)$.

COHOMOLOGICAL INVARIANTS

Γ a (finite or profinite) group, set $H^n(\Gamma) = H^n(\Gamma, \mathbf{Z}/2\mathbf{Z})$.

$H^n(k) = H^n(\Gamma_k)$.

Cohomological invariants :

L a G-Galois algebra, corresponding to

$$\phi : \Gamma_k \to G.$$

We obtain

$$\phi^* : H^n(G) \to H^n(k)$$

H^1-INVARIANTS

L a G-Galois algebra, $\phi : \Gamma_k \to G$.

$$\phi^* : H^1(G) \to H^1(k)$$

$$x \mapsto x_L$$

H^1-INVARIANTS

L a G-Galois algebra, $\phi : \Gamma_k \to G$.

$$\phi^* : H^1(G) \to H^1(k)$$
$$x \mapsto x_L$$

Proposition. L has a self-dual normal basis $\implies$ $x_L = 0$ for all $x \in H^1(G)$.

H^1-INVARIANTS

L a G-Galois algebra, $\phi : \Gamma_k \to G$.

$$\phi^* : H^1(G) \to H^1(k)$$

$$x \mapsto x_L$$

Proposition. L has a self-dual normal basis $\implies$ $x_L = 0$ for all $x \in H^1(G)$.

H^1-CONDITION :

$$x_L = 0 \text{ for all } x \in H^1(G).$$

H^1-CONDITION

$$x_L = 0 \text{ for all } x \in H^1(G).$$

Theorem. (E.B. - Serre, 1994) : Assume that $\mathrm{cd}_2(k) \leq 1$. Then

$$L \text{ has a self-dual normal basis} \iff \text{the } H^1\text{-condition holds.}$$

H^1-CONDITION

$$x_L = 0 \text{ for all } x \in H^1(G).$$

Theorem. (E.B. - Serre, 1994) : Assume that $\mathrm{cd}_2(k) \leq 1$. Then

L has a self-dual normal basis $\iff$ the H^1-condition holds.

E.B. - Parimala : Define H^2-invariants, H^2-condition.

H^1-CONDITION

$$x_L = 0 \text{ for all } x \in H^1(G).$$

Theorem. (E.B. - Serre, 1994) : Assume that $\mathrm{cd}_2(k) \leq 1$. Then

$$L \text{ has a self-dual normal basis } \iff \text{ the } H^1\text{-condition holds.}$$

E.B. - Parimala : Define H^2-invariants, H^2-condition.

Theorem. (E.B. - Parimala, 2017) : Assume that $\mathrm{cd}_2(k) \leq 2$.

$$L \text{ has a self-dual normal basis } \iff \text{ the } H^1\text{-condition holds and the } H^2\text{-condition holds.}$$

COHOMOLOGICAL REFORMULATION

$\sigma : k[G] \to k[G]$ the canonical involution of $k[G]$,

$$\sigma(g) = g^{-1} \text{ for all } g \in G.$$

U_G : linear algebraic group

$$U_G(E) = \{x \in E[G] \mid x\sigma(x) = 1\}$$

for all commutative k-algebras E.

L a G-Galois algebra

$$\Gamma_k \longrightarrow G \to U_G(k_s)$$

$$u(L) \in H^1(k, U_G).$$

COHOMOLOGICAL REFORMULATION

$$u(L) \in H^1(k, U_G).$$

$$L \text{ has a self-dual normal basis} \iff u(L) = 0.$$

$U_G = ?$

$k[G]/(\mathit{radical})$ = product of simple algebras, stable or exchanged by σ.

$$A \text{ simple algebra, } \sigma(A) = A.$$

- $\sigma \mid$ (center of A) = identity.

Then A is either orthogonal or symplectic. Set E_A = center of A.

COHOMOLOGICAL REFORMULATION

- $\sigma \mid (\text{center of } A) \neq$ identity.

Then A is unitary. Set $F_A =$ center of A, and let E_A be the fixed field of σ in F_A.

In both cases, U_A is a linear algebraic group over E_A.

$$H^1(k, U_G) = \prod_A H^1(E_A, U_A)$$

$$u(L) \mapsto (u_A(L)).$$

STRATEGY

L a G-Galois algebra, $\phi : \Gamma_k \to G$.

• Assume that the H^1-condition holds. This implies $\phi(\Gamma_k) \subset G^2$. Set

$$H = \phi(\Gamma_k).$$

• Define H^2-invariants, as follows :

• For each orthogonal and unitary factor A, define $e_A \in H^2(H)$.

• Apply $\phi^* : H^2(H) \to H^2(k)$.

ORTHOGONAL

A an orthogonal factor, U_A.

ORTHOGONAL

A an orthogonal factor, U_A.

U_A^0 : connected component of the identity, $\tilde{U}_A$: Spin group,

$$1 \to C_2 \to \tilde{U}_A \xrightarrow{s} U_A^0 \to 1.$$

ORTHOGONAL

A an orthogonal factor, U_A.

U_A^0 : connected component of the identity, $\tilde{U}_A$: Spin group,

$$1 \to C_2 \to \tilde{U}_A \xrightarrow{s} U_A^0 \to 1.$$

L a G-Galois algebra, $\phi : \Gamma_k \to G$. Assume H^1-condition. Set

$$H = \phi(\Gamma_k).$$

Define

$$e_A \in H^2(H)$$

ORTHOGONAL

$$V_A = \tilde{U}_A(E_A) \times_{U_A^0(E_A)} H,$$

central extension

$$1 \to C_2 \to V_A \ \to \ H \to 1,$$

gives

$$e_A \in H^2(H).$$

ORTHOGONAL

$\phi^* : H^2(H) \to H^2(k)$. Set

$$c_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

ORTHOGONAL

$\phi^* : H^2(H) \to H^2(k)$. Set

$$c_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

Clifford invariant of q_L at A :

$$clif_A(q_A) \in \mathrm{Br}_2(E_A)/ < A > .$$

ORTHOGONAL

$\phi^* : H^2(H) \to H^2(k)$. Set

$$c_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

Clifford invariant of q_L at A :

$$clif_A(q_A) \in \mathrm{Br}_2(E_A)/ < A > .$$

$$Res_{E_A/k} : H^2(k) \to H^2(E_A) \simeq \mathrm{Br}_2(E_A)$$

ORTHOGONAL

$\phi^* : H^2(H) \to H^2(k)$. Set

$$c_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

Clifford invariant of q_L at A :

$$clif_A(q_A) \in \mathrm{Br}_2(E_A)/ < A > .$$

$$Res_{E_A/k} : H^2(k) \to H^2(E_A) \simeq \mathrm{Br}_2(E_A)$$

Theorem. The image of $c_A(L)$ in $\mathrm{Br}_2(E_A)/ < A >$ is $clif_A(q_A)$.

ORTHOGONAL

$$Res_{E_A/k} : H^2(k) \to H^2(E_A) \simeq \mathrm{Br}_2(E_A)$$

Theorem. The image of $c_A(L)$ in $\mathrm{Br}_2(E_A)/ < A >$ is $clif_A(q_A)$.

ORTHOGONAL

$$Res_{E_A/k} : H^2(k) \to H^2(E_A) \simeq \mathrm{Br}_2(E_A)$$

Theorem. The image of $c_A(L)$ in $\mathrm{Br}_2(E_A)/ < A >$ is $clif_A(q_A)$.

L has self-dual normal basis $\implies$

$$Res_{E_A/k}(c_A(L)) = 0 \text{ in } \mathrm{Br}_2(E_A)/ < A >.$$

UNITARY

A a unitary factor, F_A : center of A.

UNITARY

A a unitary factor, F_A : center of A.

$F_A^1 = \{x \in F_A^\times \mid x\sigma(x) = 1\}$,

$$s : F_A^1 \to F_A^1$$

$$x \mapsto x^2.$$

UNITARY

A a unitary factor, F_A : center of A.

$F_A^1 = \{x \in F_A^\times \ | x\sigma(x) = 1\}$,

$$s : F_A^1 \to F_A^1$$

$$x \mapsto x^2.$$

L a G-Galois algebra, $\phi : \Gamma_k \to G$. Assume H^1-condition. Set

$$H = \phi(\Gamma_k).$$

Define

$$e_A \in H^2(H)$$

UNITARY

$$V_A = F_A^1 \times_{F_A^1} H,$$

central extension

$$1 \to C_2 \to V_A \ \to \ H \to 1,$$

gives

$$e_A \in H^2(H).$$

UNITARY

$$d_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

UNITARY

$$d_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

$$Res_{E_A/k}(d_A(L)) = disc_A(q_L) \in H^2(E_A).$$

UNITARY

$$d_A(L) = \phi^*(e_A) \in H^2(k).$$

Invariant of L, not necessarily of the trace form q_L.

$$Res_{E_A/k}(d_A(L)) = disc_A(q_L) \in H^2(E_A).$$

L has self-dual normal basis $\implies$

$$Res_{E_A/k}(d_A(L)) = 0.$$

H^2-CONDITION

$$Res_{E_A/k}(c_A(L)) = 0 \text{ in } \mathrm{Br}_2(E_A)/ < A > \text{ for all orthogonal } A,$$

and

$$Res_{E_A/k}(d_A(L)) = 0 \text{ for all unitary } A.$$

H^2-CONDITION

$$Res_{E_A/k}(c_A(L)) = 0 \text{ in } \mathrm{Br}_2(E_A)/ < A > \text{ for all orthogonal } A,$$

and

$$Res_{E_A/k}(d_A(L)) = 0 \text{ for all unitary } A.$$

L has self-dual normal basis $\implies$ H^2-condition hold.

Theorem. (E.B. - Parimala, 2017) : Assume that $\mathrm{cd}_2(k) \leq 2$.

L has a self-dual normal basis $\iff$ the H^1-condition holds and the H^2-condition holds.

Theorem. (E.B. - Parimala, 2017) : Assume that $\mathrm{cd}_2(k) \leq 2$.

L has a self-dual normal basis $\iff$ the H^1-condition holds and the H^2-condition holds.

Theorem. (E.B. - Parimala, 2017) : If G is abelian, then

L has a self-dual normal basis $\iff$ the H^1-condition holds and the H^2-condition holds.

(i) L has a self-dual normal basis;

(ii) $x_L = 0$ for all $x \in H^n(G)$, all $n > 0$.

(i) L has a self-dual normal basis;

(ii) $x_L = 0$ for all $x \in H^n(G)$, all $n > 0$.

- If $\mathrm{cd}_2(k) \leq 1$, we have (i) $\iff$ (ii).

(i) L has a self-dual normal basis;

(ii) $x_L = 0$ for all $x \in H^n(G)$, all $n > 0$.

- If $\mathrm{cd}_2(k) \leq 1$, we have (i) $\iff$ (ii).
- If $\mathrm{cd}_2(k) \leq 2$, there are examples with (i) but not (ii).

(i) L has a self-dual normal basis;

(ii) $x_L = 0$ for all $x \in H^n(G)$, all $n > 0$.

- If $\mathrm{cd}_2(k) \leq 1$, we have (i) $\iff$ (ii).
- If $\mathrm{cd}_2(k) \leq 2$, there are examples with (i) but not (ii).
- If $\mathrm{cd}_2(k) \leq 3$, there are examples with (ii) but not (i),

G quaternionian of order 8.

Invariant in $H^3(k)$, not x_L.

COHOMOLOGICAL DIMENSION 2

Assume that $\mathrm{cd}_2(k) \leq 2$.

$x_L = 0$ for all $x \in H^1(G)$ and for all $x \in H^2(H) \implies L$ has a self-dual normal basis.

COHOMOLOGICAL DIMENSION 2

Assume that $\mathrm{cd}_2(k) \leq 2$.

$x_L = 0$ for all $x \in H^1(G)$ and for all $x \in H^2(H) \implies L$ has a self-dual normal basis.

Question. $x_L = 0$ for all $x \in H^1(G)$ and for all $x \in H^2(G) \implies L$ has a self-dual normal basis ?

COHOMOLOGICAL DIMENSION 2

Assume that $\mathrm{cd}_2(k) \leq 2$.

$x_L = 0$ for all $x \in H^1(G)$ and for all $x \in H^2(H) \implies L$ has a self-dual normal basis.

Question. $x_L = 0$ for all $x \in H^1(G)$ and for all $x \in H^2(G) \implies L$ has a self-dual normal basis ?

Theorem. (E.B. - Serre, 1994) $H^1(G) = H^2(G) = 0 \implies L$ has a self-dual normal basis.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4 + 1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4 + 1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_2}^{C_8}(K)$, with K/k quadratic extension; $K = k(\sqrt{z})$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_2}^{C_8}(K)$, with K/k quadratic extension; $K = k(\sqrt{z})$.

$d_A(L) = (z)(-1) \in H^2(k)$, $Res_{E_A/k}(d_A(L)) = (z)(-1) \in H^2(E_A)$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4 + 1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_2}^{C_8}(K)$, with K/k quadratic extension; $K = k(\sqrt{z})$.

$d_A(L) = (z)(-1) \in H^2(k)$, $Res_{E_A/k}(d_A(L)) = (z)(-1) \in H^2(E_A)$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_2}^{C_8}(K)$, with K/k quadratic extension; $K = k(\sqrt{z})$.

$d_A(L) = (z)(-1) \in H^2(k)$, $Res_{E_A/k}(d_A(L)) = (z)(-1) \in H^2(E_A)$.

$$d_A(L) = 0 \iff z \text{ is a sum of two squares in } k,$$

$$\mathrm{Res}_{E_A/k}(d_A(L)) = 0 \iff z \text{ is a sum of two squares in } E_A = k(\sqrt{2}).$$

L has a self-dual normal basis $\iff$ z is a sum of two squares in $k(\sqrt{2})$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4 + 1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_4}^{C_8}(K)$, with K/k cyclic extension of degree 4.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_4}^{C_8}(K)$, with K/k cyclic extension of degree 4.

$a, b, c, \epsilon \in k$ with $a^2 - b^2\epsilon = c^2\epsilon$, $c \neq 0$, ϵ not a square.

$$x = \sqrt{\epsilon},\ K = k(\sqrt{a+bx}).$$

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_4}^{C_8}(K)$, with K/k cyclic extension of degree 4.

$a, b, c, \epsilon \in k$ with $a^2 - b^2\epsilon = c^2\epsilon$, $c \neq 0$, ϵ not a square.

$$x = \sqrt{\epsilon},\ K = k(\sqrt{a+bx}).$$

$d_A(L) = (-1)(a) + (2)(\epsilon)$, $\mathrm{Res}_{E_A/k}(d_A(L)) = \mathrm{Res}_{k(\sqrt{2})/k}((-1)(a))$.

EXAMPLE

$G = C_8$ cyclic group of order 8,

k does not contain the 4th roots of unity.

$A = k[X]/(X^4+1)$ unitary, $F_A = A$, $E_A = k(\sqrt{2})$.

$L = \mathrm{Ind}_{C_4}^{C_8}(K)$, with K/k cyclic extension of degree 4.

$a, b, c, \epsilon \in k$ with $a^2 - b^2\epsilon = c^2\epsilon$, $c \neq 0$, ϵ not a square.

$$x = \sqrt{\epsilon},\ K = k(\sqrt{a+bx}).$$

$d_A(L) = (-1)(a) + (2)(\epsilon)$, $\mathrm{Res}_{E_A/k}(d_A(L)) = \mathrm{Res}_{k(\sqrt{2})/k}((-1)(a))$.

L has a self-dual normal basis $\iff$ a is a sum of two squares in $k(\sqrt{2})$.

LOCAL FIELDS

Assume that k is a local field.

L has a self-dual normal basis $\iff$ the H^1-condition holds, and

(i) For all orthogonal A such that $[E_A : k]$ is odd and A is split, we have $c_A(L) = 0$ in $\mathrm{Br}_2(k)$.

(ii) For all unitary A such that $[E_A : k]$ is odd, we have $d_A(L) = 0$ in $\mathrm{Br}_2(k)$.

GLOBAL FIELDS

E.B - Parimala - Serre (2013) : The Hasse principle holds for the existence of self-dual normal bases.

Thank you