



ACADÉMIE  
DES SCIENCES  
INSTITUT DE FRANCE

# *Comptes Rendus*

---

# *Mathématique*

Ashish Gupta and Sugata Mandal

**Skew-Forms and Galois Theory**

Volume 362 (2024), p. 1337-1347

Online since: 14 November 2024

<https://doi.org/10.5802/crmath.645>



This article is licensed under the  
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.  
<http://creativecommons.org/licenses/by/4.0/>



*The Comptes Rendus. Mathématique are a member of the  
Mersenne Center for open scientific publishing*  
[www.centre-mersenne.org](http://www.centre-mersenne.org) — e-ISSN : 1778-3569



Research article / *Article de recherche*  
Algebra / *Algèbre*

# Skew-Forms and Galois Theory

## *Formes asymétriques et théorie de Galois*

Ashish Gupta <sup>\*,a</sup> and Sugata Mandal <sup>✉,a</sup>

<sup>a</sup> School of Mathematical Sciences, Ramakrishna Mission Vivekananda Educational and Research Institute, Belur Math, Howrah, West Bengal, Box: 711202, India.

E-mails: a0gupt@gmail.com, gmandal1961@gmail.com

**Abstract.** Let  $L/K$  be a cyclic extension of degree  $n = 2m$ . It is known that the space  $\text{Alt}_K(L)$  of alternating  $K$ -bilinear forms (skew-forms) on  $L$  decomposes into a direct sum of  $K$ -subspaces  $A^{\sigma^i}$  indexed by the elements of  $\text{Gal}(L/K) = \langle \sigma \rangle$ . It is also known that the components  $A^{\sigma^i}$  can have nice constant-rank properties. We enhance and enrich these constant-rank results and show that the component  $A^\sigma$  often decomposes directly into a sum of constant rank subspaces, that is, subspaces all of whose non-zero skew-forms have a fixed rank  $r$ . In particular, this is always true when  $-1 \notin L^2$ . As a result we deduce a decomposition of  $\text{Alt}_K(L)$  into subspaces of constant rank in several interesting situations. We also establish that a subspace of dimension  $\frac{n}{2}$  all of whose nonzero skew-forms are non-degenerate can always be found in  $A^{\sigma^i}$  where  $\sigma^i$  has order divisible by 2.

**Résumé.** Soit  $L/K$  une extension cyclique de degré  $n = 2m$ . On sait que l'espace  $\text{Alt}_K(L)$  des formes bilinéaires  $K$ -formes bilinéaires alternées (skew-forms) sur  $L$  se décompose en une somme directe de  $K$ -sous-espaces  $A^{\sigma^i}$  indexés par les éléments de  $\text{Gal}(L/K) = \langle \sigma \rangle$ . Il est également connu que les composantes  $A^{\sigma^i}$  peuvent avoir de belles propriétés de rang constant. Nous améliorons et enrichissons ces résultats de rang constant et montrons que la composante  $A^\sigma$  se décompose souvent directement en une somme de sous-espaces de rang constant, c'est-à-dire des sous-espaces dont toutes les formes asymétriques non nulles ont un rang fixe  $r$ . En particulier, ceci est toujours vrai lorsque  $-1 \notin L^2$ . En conséquence, nous déduisons une décomposition de  $\text{Alt}_K(L)$  en sous-espaces de rang constant dans plusieurs situations intéressantes. Nous établissons également qu'un sous-espace de dimension  $\frac{n}{2}$  dont toutes les formes asymétriques non nulles sont non dégénérées peut toujours être trouvé dans  $A^{\sigma^i}$  où  $\sigma^i$  a un ordre divisible par 2.

**Keywords.** Alternating form, skew-symmetric form, constant rank space, Galois extension.

**Mots-clés.** Forme alternée, forme antisymétrique, espace de rang constant, extension de Galois.

**2020 Mathematics Subject Classification.** 12F05, 12F10, 15A63.

**Funding.** The second author gratefully acknowledges support from an NBHM research award.

*Manuscript received 5 October 2023, revised and accepted 22 April 2024.*

---

\*Corresponding author

### 1. Introduction

Let  $K$  be a field of characteristic other than two and  $\text{Alt}_K(V)$  denote the space of all alternating bilinear forms (skew-forms) on a  $K$ -space  $V$  of dimension  $n$ . Suppose  $K$  admits a Galois extension  $L$  of degree  $n$ . Taking the  $n$ -dimensional  $K$ -space  $L$  as a model for  $V$  it was shown in [6] that ideas from Galois Theory can be fruitfully applied for studying skew-forms on  $V$ . Notably, this approach sheds light on the subspaces of  $\text{Alt}_K(V)$  whose nonzero skew-forms all have the same rank equal to  $k$ , say. Such “ $k$ -subspaces” besides being interesting in their own right play an important role in coding theory (see [3],[2]). Of particular importance are the  $n$ -subspaces of  $\text{Alt}_K(V)$ , that is, subspaces all of whose nonzero skew-forms are non-degenerate.

Replacing  $V$  by the  $K$ -space  $L$ , we begin with some definitions and facts given in [6, Lemma 2]. For each  $\sigma \in G := \text{Gal}(L/K)$  and  $b \in L$  we may define the skew-form

$$f_{b,\sigma}(x, y) = \text{Tr}_K^L(b(x\sigma(y) - \sigma(x)y)), \quad \forall x, y \in L. \tag{1}$$

where  $\text{Tr}_K^L : L \rightarrow K$  is the Galois-theoretic trace map defined by

$$\text{Tr}_K^L(a) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma(a), \quad \forall a \in L.$$

With each  $\sigma \in G$  we can thus associate a subspace  $A^\sigma$  of  $\text{Alt}_K(L)$  defined as  $A^\sigma := \{f_{b,\sigma} : b \in L\}$ . Each  $A^\sigma$  has dimension  $n$  unless  $\sigma$  has order 2 (see [6, Theorem 1]). It was shown in [6] that  $\text{Alt}(L)$  decomposes as a direct sum of the spaces  $A^\sigma$  with  $\sigma$  ranging over the elements of the Galois group  $G$  (see Theorems 1 and 2 below).

Let  $\text{ord}(\sigma)$  denote the order of  $\sigma \in G$ . Interestingly, for  $n$  odd, each  $A^\sigma$  is an  $n - n/\text{ord}(\sigma)$ -subspace (Theorem 1). However when  $n$  is even the situation is less clear as in this case we only know that the subspace  $A^\sigma$  has a constant rank property only when  $\sigma$  is either an involution or else it has odd order (see Section 2). When  $\sigma$  has even order it is only known that a skew form  $f_{b,\sigma} \in A^\sigma$  may have rank either  $n$  or  $n - 2n/\text{ord}(\sigma)$  and that both of these values are attained as ranks of suitable skew forms in  $A^\sigma$ . We study this last case more closely here and show that there are constant-rank subspaces in  $A^\sigma$ . In fact,  $A^\sigma$  always has an  $n$ -subspace of dimension  $\frac{n}{2}$  and moreover decomposes as a direct sum of  $k$ -subspaces for suitable  $k$  (see Theorems A-D).

**Theorem 1 ([6]).** *Suppose that  $n = [L : K]$  is odd and the Galois group  $G = \{1, \sigma_1, \dots, \sigma_m, \sigma_1^{-1}, \dots, \sigma_m^{-1}\}$  where  $m = (n - 1)/2$ . Then there is a direct decomposition*

$$\text{Alt}_K(L) = A^1 \oplus A^2 \oplus \dots \oplus A^m, \tag{2}$$

where  $A^i := A^{\sigma_i}$  has dimension  $n$  ( $1 \leq i \leq m$ ). Moreover, if  $\text{ord}(\sigma_i) = 2r_i + 1$ , the non zero skew-forms in  $A^i$  all have rank  $n - \frac{n}{2r_i + 1}$ .

**Theorem 2.** ([6]) *Suppose that  $n = [L : K]$  is even and the Galois group*

$$G = \{1, \tau_1, \dots, \tau_k, \sigma_1, \dots, \sigma_m, \sigma_1^{-1}, \dots, \sigma_m^{-1}\},$$

where  $\{\tau_1, \tau_2, \dots, \tau_k\}$  are the involutions of  $G$ , then there is a direct decomposition

$$\text{Alt}_K(L) = B^1 \oplus B^2 \oplus \dots \oplus B^k \oplus A^1 \oplus A^2 \oplus \dots \oplus A^m. \tag{3}$$

where  $B^i := A^{\tau_i}$  is an  $n$ -subspace of dimension  $n/2$  for all  $1 \leq i \leq k$  and  $A^j := A^{\sigma_j}$  ( $1 \leq j \leq m$ ) has dimension  $n$ . Moreover if  $\text{ord}(\sigma_i)$  is odd then  $A^\sigma$  is an  $n - n/\text{ord}(\sigma_i)$ -subspace of dimension  $n$ .

If  $L/K$  is cyclic Galois extension of degree  $n$  with  $G = \text{Gal}(L/K) = \langle \sigma \rangle$  we define  $A^i := A^{\sigma^i}$ . Thus  $A^i = \{f_{b,\sigma^i} : b \in L\}$ . If  $n$  is even then there is a unique involution  $\tau_1 = \sigma^{n/2}$  and in this case we denote  $B^1 := A^{\tau_1} = \{f_{b,\sigma^{n/2}} : b \in L\}$ . Then the decomposition (3) becomes

$$\text{Alt}_K(L) = B^1 \oplus A^1 \oplus A^2 \oplus \dots \oplus A^m, \tag{4}$$

**Theorem A.** Let  $K$  be a field and  $n = 2k$ , where  $k \geq 1$  is odd. Let  $L$  be any cyclic extension of  $K$  of degree  $n$  with Galois group  $G = \langle \sigma \rangle$ . Then

$$A^1 = \mathcal{U}_1 \oplus \mathcal{V}_1, \tag{5}$$

where  $\mathcal{U}_1$  is an  $n$ -subspace of dimension  $k$  and  $\mathcal{V}_1$  is an  $(n - 2)$ -subspace of dimension  $k$ .

In view of Theorem A in the following theorems we focus on the case where  $n$  is divisible by 4.

**Theorem B.** Suppose  $n = 2^\alpha k$  where  $\alpha \geq 2$  and  $k$  is odd. Let  $K$  be an algebraic number field such that  $-1$  is not a square in  $K$ . Then there exists a cyclic extension  $L$  of  $K$  of degree  $n$  with the Galois group  $G = \langle \sigma \rangle$  such that

$$A^1 = \mathcal{E}_1 \oplus \cdots \oplus \mathcal{E}_{\alpha-1} \oplus \mathcal{V}_1 \oplus \mathcal{V}_2, \tag{6}$$

where

- (i)  $\mathcal{E}_i$  is an  $n$ -subspace of dimension  $n/2^i$  for  $1 \leq i \leq \alpha - 1$ ,
- (ii)  $\mathcal{V}_j$  is an  $(n - 2)$ -subspace of dimension  $k$  for  $1 \leq j \leq 2$ .

**Theorem C.** Let  $K$  be a finite field with  $q$  elements such that  $-1$  is not a square in  $K$ . Let  $q + 1 = 2^a l$  ( $l$  odd) where  $a \geq 1$  and  $n = 2^\alpha k$  ( $k$  odd) where  $\alpha \geq 2$ . Suppose  $L$  is a cyclic extension of  $K$  of degree  $n$  with  $\text{Gal}(L/K) = \langle \sigma_f \rangle$  where  $\sigma_f$  is the Frobenius map of  $L$  defined by  $\sigma_f : b \rightarrow b^q$ .

- (1) If  $\alpha \leq a + 1$  then

$$A^1 = \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus \mathcal{E}_1 \oplus \cdots \oplus \mathcal{E}_{\alpha-1}, \tag{7}$$

where

- (i)  $\mathcal{E}_i$  is an  $n$ -subspace of dimension  $n/2^i$  for  $1 \leq i \leq \alpha - 1$ ,
  - (ii)  $\mathcal{V}_j$  is an  $(n - 2)$ -subspace of dimension  $k$  for  $1 \leq j \leq 2$ .
- (2) If  $\alpha > a + 1$  and  $l = 1$ , that is,  $q = 2^a - 1$ , then

$$A^1 = \mathcal{V}_1 \oplus \mathcal{V}_2 \oplus \mathcal{E}_1 \oplus \cdots \oplus \mathcal{E}_{\alpha-1}, \tag{8}$$

where

- (i)  $\mathcal{E}_i$  is an  $n$ -subspace of dimension  $n/2^i$  for  $1 \leq i \leq a$  and an  $(n - 2)$ -subspace of dimension  $n/2^i$  for  $a + 1 \leq i \leq \alpha - 1$ ,
- (ii)  $\mathcal{V}_j$  is an  $(n - 2)$ -subspace of dimension  $k$  for  $1 \leq j \leq 2$ .

**Theorem D.** Let  $p$  be a prime and  $K = \mathbb{Q}_p$  be the  $p$ -adic completion of  $\mathbb{Q}$  such that  $-1$  is not a square in  $K$ . Let  $p + 1 = 2^a l$  ( $l$  odd) where  $a \geq 1$  and  $n = 2^\alpha k$  ( $k$  odd) where  $2 \leq \alpha \leq a + 1$ . Then there exists a cyclic extension  $L$  of  $K$  of degree  $n$  such that the decomposition (7) holds.

## 2. Skew forms and Galois extensions

Retaining the notation of the previous section we now collect some basic results from [6] concerning the application of Galois theory to the study of some crucial properties of bilinear forms over  $K$ . In the following  $L/K$  is a (not necessarily cyclic) Galois extension and  $1 \neq \sigma \in \text{Gal} L/K$  is arbitrary.

**Lemma 1 ([6, Lemma 2]).** Let  $f = f_{b,\sigma}$  be an alternating bilinear form as defined above with  $b \neq 0$  and let  $F$  be the fixed field of the automorphism  $\sigma^2$ . If  $\sigma(b)b^{-1}$  is expressible in the form  $\sigma^2(c)c^{-1}$  for some  $c \in L^\times$  then  $\text{rk}(f_{b,\sigma}) = n - n/[L : F]$ . Otherwise  $\text{rk}(f_{b,\sigma}) = n$ .

**Lemma 2 ([6, Lemma 4]).** Suppose that the automorphism  $\sigma$  has even multiplicative order  $2r$ , say. Then there exist elements  $b \in L^\times$  such that the equation  $\sigma(b)b^{-1} = \sigma^2(c)c^{-1}$  has no solution for all  $c \in L^\times$ .

**Remark 3.** If  $\sigma$  is not an involution then the map  $b \rightarrow f_{b,\sigma}$  defines an isomorphism of  $K$ -spaces between  $A^\sigma$  and  $L$  [6, Theorem 1].

**Lemma 4 ([6, Lemma 3]).** *Suppose that the automorphism  $\sigma$  has odd multiplicative order  $2r + 1 > 1$ , say. Then, if  $b \neq 0$ , the rank of the skew-form  $f = f_{b,\sigma}$  is  $n - n/2r + 1$ .*

**Lemma 5 ([6, Lemma 4]).** *Suppose that the automorphism  $\sigma$  has even multiplicative order  $2r \geq 2$ , say. Then, if  $b \neq 0$ , the rank of the skew-form  $f = f_{b,\sigma}$  is either  $n - \frac{n}{r}$  or  $n$ .*

### 3. Preliminary results

Our aim in this section is to establish certain facts which will be found useful in the subsequent sections and are also interesting in their own right. Recall that if  $F$  is an intermediate subfield and  $a \in L$  then the  $L/F$ -norm  $N_{L/F}(a)$  of  $a$  is defined as  $N_{L/F}(a) = \prod_{\theta \in \text{Gal}(L/F)} \theta(a)$ .

**Notation 6.** Throughout this section  $L/K$  denotes a cyclic extension with Galois group  $\text{Gal}(L/K) = \langle \sigma \rangle$ . For the sake of convenience in what follows we shall denote the subfield  $L^{\langle \sigma^i \rangle}$  as  $L_i$ .

We begin by noting the following restatement of the degeneracy criterion Lemma 1.

**Proposition 7.** *Let  $b \in L$ . Then the skew-form  $f_{b,\sigma}$  is degenerate if and only if*

$$N_{L/L_2}(\sigma(b)/b) = 1, \tag{9}$$

*that is,  $f_{b,\sigma}$  is degenerate if and only if*

$$N_{L/L_2}(b) = b\sigma^2(b) \cdots \sigma^{n-2}(b) \in K. \tag{10}$$

**Proof.** By Lemma 1, the skew form  $f_{b,\sigma}$  is degenerate if and only if  $\sigma(b)/b = \sigma^2(c)/c$  for some  $c \in L$ . The first assertion is now clear in view of the Hilbert Theorem 90. Moreover the condition  $N_{L/L_2}(\sigma(b)/b) = 1$  is easily seen to be equivalent to the product  $b\sigma^2(b) \cdots \sigma^{n-2}(b)$  being  $\sigma$ -invariant. □

Suppose that  $\sigma^i$  is not an involution. By Lemma 1 the skew-form  $f_{b,\sigma^i} \in A^i \subseteq \text{Alt}_K(L)$  is degenerate if and only if  $\sigma^i(b)/b = \sigma^{2i}(c)/c$ . As  $\sigma^{2i}$  is a generator for  $\text{Gal}(L/L_{2i})$ , in view of Hilbert Theorem 90,  $f_{b,\sigma^i}$  is degenerate if and only if  $N_{L/L_{2i}}(\sigma^i(b)/b) = 1$ . A glance at Proposition 7 above shows that this is precisely the condition for the skew-form  $f_{b,\sigma^i}^{\sim} \in \text{Alt}_{L_i}(L)$  defined by

$$f_{b,\sigma^i}^{\sim} = \text{Tr}_{L_i}^L(b(x\sigma(y) - \sigma(x)y)), \quad \forall x, y \in L.$$

to be degenerate (we write  $f_{b,\sigma^i}^{\sim}$  instead of  $f_{b,\sigma^i}$  to emphasize the fact that we are now considering  $L$  as  $L_i$ -space).

Let us write  $A^{\sim 1} := \{f_{b,\sigma^i}^{\sim} \mid b \in L\}$ . In view of Remark 3 we then have a  $K$ -isomorphism  $A^i \cong L$  via  $f_{b,\sigma^i} \mapsto b$  and an  $L_i$ -isomorphism  $L \cong A^{\sim 1}$  via  $b \mapsto f_{b,\sigma^i}^{\sim}$ . The composition of these maps clearly yields a  $K$ -isomorphism  $A^i \cong A^{\sim 1}$ . The following is then clear.

**Remark 8.** With respect to the above isomorphism if an  $L_i$ -subspace  $\mathcal{W} \leq A^{\sim 1}$  has all its non-zero skew forms non-degenerate (or all its non-zero skew forms degenerate) then the same is true for the corresponding ( $K$ -) subspace in  $A^i$ .

**Lemma 9.** *Let  $n = 2^\alpha k$  where  $\alpha \geq 2$  and  $k$  is odd. Suppose that  $L$  is a cyclic extension of a field  $K$  of degree  $n$  with Galois group  $\text{Gal}(L/K) = \langle \sigma \rangle$ . Then the following hold.*

- (i) *For  $1 \leq i \leq \alpha - 1$  the subspace  $E_i := \{b \in L : \sigma^{n/2^i}(b) = -b\} \leq L$  has dimension  $n/2^i$ .*
- (ii) *Let  $V_1 := \{b \in L : \sigma^k(b) = b\}$  and  $V_2 := \{b \in L : \sigma^k(b) = -b\}$ . Then  $\dim(V_1) = \dim(V_2) = k$ .*

**Proof.** Let  $1 \leq i \leq \alpha - 1$ . As the order of the automorphism  $\sigma^{n/2^i}$  is  $2^i$  so the fixed field  $L_{n/2^i}$  of  $\sigma^{n/2^i}$  has dimension  $n/2^i$  over  $K$ . We can view  $\sigma^{n/2^i}$  as a  $K$ -linear map of  $L$ . By the Dedekind independence theorem the minimal polynomial of  $\sigma^{n/2^i}$  is  $x^{2^i} - 1$ . Let  $j_i \in L$  be an eigenvector of  $\sigma^{n/2^i}$  corresponding to the eigenvalue  $-1$ . It is easily checked that the corresponding eigenspace is  $E_i := j_i L_{n/2^i}$ . It follows that  $\dim(E_i) = n/2^i$ . The proof of (ii) is similar.  $\square$

**Lemma 10.** Let  $n = 2^\alpha k$  where  $\alpha \geq 2$  and  $k$  is odd. Suppose that  $L$  is a cyclic extension of a field  $K$  of degree  $n$  with Galois group  $\text{Gal}(L/K) = \langle \sigma \rangle$ . Then  $\forall b_i \in E_i \setminus \{0\}$

$$N_{L/L_2}(b_i) = (-1)^{n/2^2} w_i^{2^i}, \tag{11}$$

where  $w_i := b_i \sigma^2(b_i) \cdots \sigma^{n/2^i - 2}(b_i)$ . Moreover,  $f_{b_i, \sigma}$  is degenerate if and only if  $\eta_i := \sigma(w_i)/w_i$  is a  $2^i$ -th root of unity in  $L$  such that  $\sigma(\eta_i) = -\eta_i^{-1}$ . In particular,  $f_{b_i, \sigma}$  is non-degenerate for all  $b_i \in E_i \setminus \{0\}$ .

**Proof.** In view of the chain of inclusions

$$L \supset L_{n/2} \supset \cdots \supset L_{n/2^{i-1}} \supset E_i,$$

we have for  $b_i \in E_i \setminus \{0\}$

$$\begin{aligned} N_{L/L_2}(b_i) &= b_i \sigma^2(b_i) \cdots \sigma^{n-2}(b_i) \\ &= (b_i \sigma^2(b_i) \cdots \sigma^{n/2-2}(b_i)) (\sigma^{n/2}(b_i) \sigma^{n/2+2}(b_i) \cdots \sigma^{n/2+n/2-2}(b_i)) \\ &= (b_i \sigma^2(b_i) \cdots \sigma^{n/2-2}(b_i))^2 \\ &= (b_i \sigma^2(b_i) \cdots \sigma^{n/4-2}(b_i))^{2^2} \\ &\quad \vdots \\ &= (b_i \sigma^2(b_i) \cdots \sigma^{n/2^{i-1}-2}(b_i))^{2^{i-1}} \\ &= \left[ (b_i \sigma^2(b_i) \cdots \sigma^{n/2^i-2}(b_i)) (\sigma^{n/2^i}(b_i) \sigma^{n/2^i+2}(b_i) \cdots \sigma^{n/2^i+n/2^i-2}(b_i)) \right]^{2^{i-1}} \\ &= \left[ (b_i \sigma^2(b_i) \cdots \sigma^{n/2^i-2}(b_i)) ((-b_i)(-\sigma^2(b_i)) \cdots (-\sigma^{n/2^i-2}(b_i))) \right]^{2^{i-1}} \\ &= \left[ (-1)^{n/2^{i+1}} (b_i \sigma^2(b_i) \cdots \sigma^{n/2^i-2}(b_i)) \right]^{2^{i-1}} \\ &= (-1)^{n/2^2} [b_i \sigma^2(b_i) \cdots \sigma^{n/2^i-2}(b_i)]^{2^i} \\ &= (-1)^{n/2^2} w_i^{2^i}. \end{aligned}$$

Then

$$\frac{N_{L/L_2}(\sigma(b_i))}{N_{L/L_2}(b_i)} = \left( \frac{\sigma((-1)^{n/2^2} w_i)}{(-1)^{n/2^2} w_i} \right)^{2^i} = \left( \frac{\sigma(w_i)}{w_i} \right)^{2^i} = \eta_i^{2^i}.$$

Set  $\eta_i := \frac{\sigma(w_i)}{w_i}$ . By Proposition 7,  $f_{b_i, \sigma}$  is degenerate if and only if  $\eta_i$  is a  $2^i$ -th root of unity  $\eta_i$ . Moreover,

$$-w_i = \sigma^2(w_i) = \sigma(\eta_i w_i) = \sigma(\eta_i) \eta_i w_i,$$

whence  $\sigma(\eta_i) \eta_i = -1$ , that is,  $\sigma(\eta_i) = -\eta_i^{-1}$ . The last assertion in the theorem is now clear.  $\square$

**Lemma 11.** Let  $n = 2^\alpha k$  where  $\alpha \geq 2$  and  $k$  is odd. Suppose that  $L$  is a cyclic extension of  $K$  of degree  $n$  with  $\text{Gal}(L/K) = \langle \sigma \rangle$ . Then  $\forall b \in V_1 \cup V_2$ ,  $f_{b, \sigma}$  is degenerate.

**Proof.**

**Case I.** Let us first assume that  $k > 1$ . Then the field  $V_1 = L_k$  has dimension  $k$  over  $K$ . Again by Dedekind's independence theorem it follows that the minimal polynomial of  $\sigma^k$  is  $x^{2^\alpha} - 1$ . Let  $j_\alpha$  be an eigenvector of  $\sigma^k$  corresponding to the eigenvalue  $-1$  and it is easily checked that the corresponding eigenspace is  $V_2 = j_\alpha L_k$ . Thus  $\dim(V_1) = \dim(V_2) = k$ . Note that  $V_1$  and  $V_2$  are  $\sigma$ -invariant. Again in view of the inclusions

$$L \supset L_{n/2} \supset \dots \supset L_{n/2^{\alpha-1}} = L_{2k} \supset L_k = V_1,$$

we have  $\forall b \in V_1 \setminus \{0\}$ ,

$$\begin{aligned} N_{L/L_2}(b) &= b\sigma^2(b) \dots \sigma^{n-2}(b) \\ &= \left( b\sigma^2(b) \dots \sigma^{n/2^{\alpha-1}-2}(b) \right)^{2^{\alpha-1}} \\ &= \left( b\sigma^2(b) \dots \sigma^{2k-2}(b) \right)^{2^{\alpha-1}} \\ &= \left[ \left( b\sigma^2(b) \dots \sigma^{k-1}(b) \right) \left( \sigma^{k+1}(b) \dots \sigma^{2k-2}(b) \right) \right]^{2^{\alpha-1}} \\ &= \left[ \left( b\sigma^2(b) \dots \sigma^{k-1}(b) \right) \left( \sigma(b) \dots \sigma^{k-2}(b) \right) \right]^{2^{\alpha-1}} \\ &= [b\sigma(b)\sigma^2(b) \dots \sigma^{k-1}(b)]^{2^{\alpha-1}} \\ &= N_{L/L_2}(\sigma(b)). \end{aligned}$$

On the other hand in view of the inclusions

$$L \supset L_{n/2} \supset \dots \supset L_{n/2^{\alpha-1}} = L_{2k} \supset j_\alpha L_k = V_2,$$

we have  $\forall b \in V_2 \setminus \{0\}$ ,

$$\begin{aligned} N_{L/L_2}(b) &= b\sigma^2(b) \dots \sigma^{n-2}(b) \\ &= \left( b\sigma^2(b) \dots \sigma^{n/2^{\alpha-1}-2}(b) \right)^{2^{\alpha-1}} \\ &= \left( b\sigma^2(b) \dots \sigma^{2k-2}(b) \right)^{2^{\alpha-1}} \\ &= \left[ \left( b\sigma^2(b) \dots \sigma^{k-1}(b) \right) \left( \sigma^{k+1}(b) \dots \sigma^{2k-2}(b) \right) \right]^{2^{\alpha-1}} \\ &= \left[ \left( b\sigma^2(b) \dots \sigma^{k-1}(b) \right) \left( (-\sigma(b)) \dots (-\sigma^{k-2}(b)) \right) \right]^{2^{\alpha-1}} \\ &= [b\sigma(b)\sigma^2(b) \dots \sigma^{k-1}(b)]^{2^{\alpha-1}} \\ &= N_{L/L_2}(\sigma(b)). \end{aligned}$$

Consequently  $N_{L/L_2}(\sigma(b)/b) = 1$  and thus by Proposition 7  $\forall b \in V_1 \cup V_2$ ,  $f_{b,\sigma}$  is degenerate.

**Case II.** We now assume that  $k = 1$  (thus  $n = 2^\alpha$  and  $L_{2k} = L_2$ ). Then  $V_1 := K$  and it is easily checked that  $V_2 := j_\alpha K$ , where  $j_\alpha$  is an eigenvector of  $\sigma$  corresponding to the eigenvalue  $-1$ . Thus  $\dim(V_1) = \dim(V_2) = 1$ . Clearly if  $b \in L_2^\times$  then  $N_{L/L_2}(b) = b^{2^{\alpha-1}}$  and  $N_{L/L_2}(\sigma(b)) = (\sigma(b))^{2^{\alpha-1}}$  as  $L_2$  is  $\sigma$ -invariant. By definition if  $b \in V_1 \cup V_2$  then  $\sigma(b) = \pm b$  and in either case

$$N_{L/L_2}\left(\frac{\sigma(b)}{b}\right) = \left(\frac{\sigma(b)}{b}\right)^{2^{\alpha-1}} = 1.$$

Thus by Proposition 7 if  $b \in V_1 \cup V_2$ ,  $f_{b,\sigma}$  is degenerate. □

#### 4. Proofs of Theorems A and B

##### 4.1. Proof of Theorem A

**Proof.** Let  $V := L_k$  and  $0 \neq v \in V$ . Clearly

$$\sigma^2(v), \sigma^4(v), \dots, \sigma^{2k-2}(v) \in V.$$

It follows that

$$N_{L/L_2}(v) \in L_2 \cap V = L_2 \cap L_k = K.$$

By Proposition 7 the skew-form  $f_{v,\sigma}$  is degenerate and by Lemma 5 it has rank  $n - 2 = 2k - 2$ .

By Lemmas 1 and 2 there exists a  $j \in L$  such that  $f_{j,\sigma}$  is non-degenerate. Then for  $0 \neq v \in V$

$$N_{L/L_2}(jv) = N_{L/L_2}(j)N_{L/L_2}(v) \notin K.$$

It thus follows by proposition 7 that all the nonzero skew-forms  $f_{b,\sigma}$  where  $b$  lies in the subspace  $U = jV$  (of dimension  $k$ ) are non-degenerate. Clearly  $U \cap V = \{0\}$  so  $L = U \oplus V$ . By Remark 3 the subspace  $U$  of  $L$  corresponds to a subspace  $\mathcal{U}$  of  $\text{Alt}_K(L)$  with the same dimension defined by  $\mathcal{U} := \{f_{b,\sigma} : b \in U\}$ . Similarly  $V$  corresponds to  $\mathcal{V} \leq \text{Alt}_K(L)$  such that  $\dim(V) = \dim(\mathcal{V})$ . Then the decomposition (5) follows.  $\square$

**Corollary 12.** *Let  $K$  be a field and  $n$  be even. Suppose  $L$  is a cyclic Galois extension of a field  $K$  of degree  $n$  with Galois group  $\text{Gal}(L/K) = \langle \sigma \rangle$ . If  $\text{ord}(\sigma^i) \equiv 2 \pmod{4}$  and  $\text{ord}(\sigma^i) \neq 2$  then*

$$A^i = \mathcal{U}_i \oplus \mathcal{V}_i,$$

where  $\mathcal{U}_i$  is an  $n$ -subspace of dimension  $n/2$  and  $\mathcal{V}_i$  is an  $(n - 2n/\text{ord}(\sigma^i))$ -subspace of dimension  $n/2$ .

**Proof.** This follows from Theorem A, noting Remark 8 and the fact (Lemma 5) that a skew form in  $A^i$  is either non-degenerate or has rank equal to  $n - 2n/\text{ord}(\sigma^i)$ .  $\square$

Consequently we obtain the following.

**Corollary 13.** *Let  $K$  be a field and  $n = 2k$ , where  $k \geq 1$  is odd. Let  $L$  be any cyclic Galois extension of  $K$  of degree  $n$  with Galois group  $G = \langle \sigma \rangle$ . Then*

$$\text{Alt}_K(L) = B^1 \oplus \left( \bigoplus_{\substack{\text{ord}(\sigma^i) \equiv 0 \pmod{2} \\ \text{ord}(\sigma^i) \neq 2}} (\mathcal{U}_i \oplus \mathcal{V}_i) \right) \oplus \left( \bigoplus_{\text{ord}(\sigma^i) \equiv 1 \pmod{2}} A^i \right) \tag{12}$$

**Proof.** Clear in view of Corollary 12, Lemma 4 as well as the decomposition (4).  $\square$

**Remark 14.** Let  $n = 2^\alpha k$  where  $\alpha \geq 1$  and  $k$  is odd. Suppose that  $L$  is a cyclic extension of a field  $K$  of degree  $n$  with Galois group  $\text{Gal}(L/K) = \langle \sigma \rangle$ . If  $\text{ord}(\sigma^i)$  is even then there always exists an  $n$ -subspace of dimension  $n/2$  inside  $A^i$ . If  $\alpha = 1$  this follows from Corollary 13. Otherwise if  $\alpha > 1$  then it follows from Lemma 10 that  $\mathcal{E}_1 := \{f_{b,\sigma} : b \in E_1\}$  is the desired subspace for  $A^1$ . The corresponding assertion for  $A^i$  now follows in the light of Remark 8.

##### 4.2. Proof of Theorem B

**Proof.** Firstly we will construct a cyclic extension  $L$  of  $K$  such that  $i \notin L$  where  $i$  is a primitive  $2^2$ -th root of unity. Let  $p$  be a prime such that  $p \equiv 1 \pmod{n}$  and consider the cyclotomic extension  $\mathbb{Q}(\eta_p)$  where  $\eta_p$  is a primitive  $p$ -th root of unity. As is known (e.g., [5, Lemma 4]) it is possible to pick the prime  $p$  as above such that  $\mathbb{Q}(\eta_p) \cap K(i) = \mathbb{Q}$ . Let  $L$  be the unique intermediate field



$\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\eta_p)$  such that  $[L : \mathbb{Q}] = n$ . Clearly  $L \cap K(i) = \mathbb{Q} = L \cap K$ . By a well known fact (e.g., [8, Chapter 6, Theorem 1.12]) the extensions  $LK(i)/K(i)$  and  $LK/K$  are Galois and

$$\text{Gal}(LK(i)/K(i)) \cong \text{Gal}(L/L \cap K(i)) = \text{Gal}(L/\mathbb{Q}) = \text{Gal}(L/L \cap K) \cong \text{Gal}(LK/K).$$

If  $i \in LK$  then by the last equation

$$[LK : K] = [LK : K(i)][K(i) : K] = [LK(i) : K(i)][K(i) : K],$$

whence  $[K(i) : K] = 1$  thus contradicting the hypothesis on  $K$ . Redefining  $L := LK$  yields the desired cyclic extension  $L/K$  with degree  $n$ .

Let  $E_i := \{b \in L : \sigma^{n/2^i}(b) = -b\}$  ( $1 \leq i \leq \alpha - 1$ ). By Lemma 9 we obtain  $L_{n/2^{i-1}} = L_{n/2^i} \oplus E_i$  and  $L_{2k} = V_1 \oplus V_2$ , where  $V_1$  and  $V_2$  denote the eigenspaces of  $\sigma^k$  with respect to the eigenvalues 1 and  $-1$  respectively. Consequently, we obtain

$$L = L_{n/2} \oplus E_1 = L_{n/4} \oplus E_2 \oplus E_1 = L_{2k} \oplus E_{\alpha-1} \oplus \dots \oplus E_1 = V_1 \oplus V_2 \oplus E_{\alpha-1} \oplus \dots \oplus E_1. \tag{13}$$

Let  $\mathcal{E}_i$  be the subspace of  $A^1$  corresponding to  $E_i := \{b \in L : \sigma^{n/2^i}(b) = -b\}$  under the isomorphism of Remark 3, that is,  $\mathcal{E}_i = \{f_{b,\sigma} : b \in E_i\}$  ( $1 \leq i \leq \alpha - 1$ ). By our construction, the only  $2^i$ -th roots in  $L$  are  $\pm 1$ . As  $\sigma$  fixes both these roots, it follows from Lemma 10 that  $\mathcal{E}_i$  is an  $n$ -subspace for all  $i$  in the above range.

Similarly, let  $\mathcal{V}_j$  correspond to the subspace  $V_j$  of  $L$ . By Lemma 11 the nonzero skew-forms in  $\mathcal{V}_j$ , where  $j = 1, 2$  are degenerate whence these are  $(n - 2)$ -spaces by Lemma 5. The required decomposition (6) is now immediate from (13).  $\square$

**Corollary 15.** *In the situation of Theorem B if  $\text{ord}(\sigma^i) \equiv 0 \pmod{4}$ , say  $\text{ord}(\sigma^i) = 2^\beta k'$  ( $\beta \geq 2$ ) then*

$$A^i = \mathcal{V}_1^i \oplus \mathcal{V}_2^i \oplus \mathcal{E}_1^i \oplus \dots \oplus \mathcal{E}_{\beta-1}^i, \tag{14}$$

where

- (i)  $\mathcal{E}_k^i$  is an  $n$ -subspace of dimension  $n/2^i$  for  $1 \leq k \leq \beta - 1$ ,
- (ii)  $\mathcal{V}_j^i$  is  $(n - 2n/\text{ord}(\sigma^i))$ -subspace of dimension  $k'n/\text{ord}(\sigma^i)$  for  $1 \leq j \leq 2$ .

**Proof.** This follows from proof of Theorem B, noting Remark 3 and the fact (Lemma 5) that a skew form in  $A^i$  is either non-degenerate or has rank equal to  $n - 2n/\text{ord}(\sigma^i)$ .  $\square$

**Corollary 16.** *In the situation of Theorem B there is direct-decomposition*

$$\text{Alt}_K(L) = B^1 \oplus \left( \bigoplus_{\substack{\text{ord}(\sigma^i) \equiv 2 \pmod{4} \\ \text{ord}(\sigma^i) \neq 2}} (\mathcal{U}_i \oplus \mathcal{V}_i) \right) \oplus \left( \bigoplus_{\text{ord}(\sigma^i) \equiv 1 \pmod{2}} A^i \right) \oplus \bigoplus_{\text{ord}(\sigma^i) \equiv 0 \pmod{4}} (\mathcal{V}_1^i \oplus \mathcal{V}_2^i \oplus \mathcal{E}_{\beta-1}^i \oplus \dots \oplus \mathcal{E}_1^i) \tag{15}$$

**Proof.** Using Corollaries 12, 15 and Lemma 4 as well as the decomposition (4), we can deduce the required decomposition.  $\square$

**Remark 17.** As its proof shows, Theorem B as well as its corollaries remain valid for an arbitrary cyclic extension  $L/K$  of degree  $n = 2^\alpha k$  ( $\alpha \geq 2$ ) such that  $-1$  is not a square in  $L$ . Similarly, let  $K$  be a field such that  $f(X) := X^4 + 1$  is irreducible in  $K[X]$  (it is not difficult to show that  $K$  has this property if and only if none of  $-1, 2$  and  $-2$  is a square in  $K$ ). Then Theorem B holds true for any cyclic extension  $L/K$  of degree  $n = 2^\alpha k$ . Indeed, if  $\eta_i$  is a  $2^i$ -root of unity for  $i \geq 1$  then the conditions  $-1 \notin K^2$  and  $\sigma(\eta_i) = -\eta_i^{-1}$  mean that  $\eta_i \notin \{\pm 1, \pm i\}$ , where  $i$  denotes a primitive 4-th root of unity in  $L$ . Thus  $\eta$  must have order  $2^s$  where  $s \geq 3$ . Since  $\eta \in L_2$  this would mean that  $L_2$  contains an element of order 8 and thus a root of  $f$  implying  $f$  has a quadratic factor in  $K[X]$ .

### 5. Proofs of Theorems C and D

#### 5.1. Proof of Theorem C

**Proof.** Let  $E_i$  ( $1 \leq i \leq \alpha - 1$ ) and  $V_j$  ( $1 \leq j \leq 2$ ) be as in Lemma 9. As in the proof of Theorem B, we have

$$L = V_1 \oplus V_2 \oplus E_{\alpha-1} \oplus \dots \oplus E_1.$$

By the hypothesis  $-1$  is not a square in  $K$  from which it easily follows that  $a \geq 2$ . Let  $w_i$  and  $\eta_i$  be as in Lemma 10. Note that  $\sigma_f^2(w_i) = -w_i$  and thus  $w_i^2 \in L_2$  but  $w_i \notin L_2$ . Consequently  $w_i^{2(q^2-1)} = 1$  and  $w_i^{(q^2-1)} = -1$ . Since  $\sigma_f(w_i) = w_i^q$  hence  $\eta_i = w_i^{q-1}$ . It follows that  $\eta_i$  is a  $2(q+1)$ -th root of unity but not a  $(q+1)$ -th root of unity.

(1). Suppose  $\alpha \leq a + 1$ . Since  $1 \leq i \leq \alpha - 1$  therefore  $1 \leq i \leq a$ . Again by Lemma 10,  $f_{b_i, \sigma_f}$  is degenerate if and only if  $\eta_i$  is a  $2^i$ -th root of unity. Since  $i \leq a$ , this would mean that  $\eta_i^{q+1} = \eta_i^{2^{a+1}} = 1$ , a contradiction. Let  $\mathcal{E}_i$  be the subspace of  $A^1$  corresponding to  $E_i$  under the isomorphism of Remark 8. It follows that  $\mathcal{E}_i$  is an  $n$ -subspace of dimension  $n/2^i$ .

(2). Suppose  $\alpha > a + 1$ . Pick  $i \in [1, \alpha - 1]$ . If  $1 \leq i \leq a$  it follows from part (1) above that  $E_i$  is an  $n$ -subspace for  $1 \leq i \leq a$ . So we assume that  $i \geq a + 1$ . By the hypothesis  $l = 1$ , whence  $\eta_i^{2^{a+1}} = \eta_i^{2^{(q+1)}} = 1$ . It follows that if  $a + 1 \leq i \leq \alpha - 1$  then  $\eta_i^{2^i} = 1$ . Thus in view of Lemma 10 all the skew-forms in  $\mathcal{E}_i$  are degenerate and in this case by Lemma 5,  $\mathcal{E}_i$  is an  $(n - 2)$ -subspace. Similarly let  $\mathcal{V}_j$  be the subspace of  $A^1$  corresponding to  $V_j$ . Then by Lemmas 11 and 5,  $\mathcal{V}_j$  is an  $(n - 2)$ -subspace. □

**Remark 18.** In Theorem C when  $\alpha > a + 1$  and  $l > 1$  then  $\mathcal{E}_i$  is neither an  $n$ -subspace nor an  $(n - 2)$ -subspace for  $a + 1 \leq i \leq \alpha - 1$ . Indeed, by the definition of  $E_i$

$$E_i = \{b \in L : \sigma_f^{n/2^i}(b) = -b\} = \{b \in L : b^{q^{n/2^i} - 1} = -1\}.$$

Let  $C := \{b \in L^\times : b^{2(q^{n/2^i} - 1)} = 1\}$ . Then  $C$  is a cyclic subgroup of  $L^\times$ . Clearly,  $C = L^{\times}_{n/2^i} \cup (E_i \setminus \{0\})$ . Let  $u$  be a generator of  $C$ . It is clear that  $b_i = u^s \in E_i$  if and only if  $s$  is odd. We claim that  $f_{b_i, \sigma_f}$  is degenerate if and only if  $s$  is an odd multiple of  $l$ . Indeed, let  $w_i$  and  $\eta_i$  be as in Lemma 10. Then

$$w_i = b_i \sigma_f^2(b_i) \dots \sigma_f^{n/2^i - 2}(b_i) = b_i b_i^{q^2} \dots b_i^{q^{n/2^i - 2}} = b_i^{\frac{q^{n/2^i} - 1}{q^2 - 1}},$$

and

$$\eta_i = w_i^{q-1} = b_i^{\frac{q^{n/2^i} - 1}{q+1}} = b_i^t,$$

where  $t := \frac{q^{n/2^i} - 1}{q+1}$ . By Lemma 10,  $f_{b_i, \sigma}$  is degenerate if and only if  $\eta_i^{2^i} = 1$ . Now from the proof of Theorem C,  $\eta_i^{2^{a+1}l} = \eta_i^{2^{(q+1)}} = 1$  and  $\eta_i^{2^{a+1}} = \eta^{(q+1)} \neq 1$ . Consequently  $f_{b_i, \sigma_f}$  is degenerate if and only if  $\eta_i$  is a primitive  $2^{a+1}$ -th root of unity, that is, if and only if,

$$2^{a+1} = \text{ord}(\eta_i) = \text{ord}(u^{st}) = \frac{\text{ord}(u)}{\text{gcd}(\text{ord}(u), st)} = \frac{2(q+1)t}{\text{gcd}(2(q+1)t, st)} = \frac{2^{a+1}l}{\text{gcd}(2^{a+1}l, s)}, \tag{16}$$

or,  $\text{gcd}(2^{a+1}l, s) = l$ . In other words, for  $b_i = u^s \in E_i$ ,  $f_{b_i, \sigma_f}$  is degenerate if and only if  $s$  is an odd multiple of  $l$ . Thus, for example,  $f_{u^l, \sigma_f}$  is degenerate while  $f_{u, \sigma_f}$  is non-degenerate.

5.2. Proof of Theorem D

**Proof.** By [4, Proposition 5.4.11] for every  $n$  there exists exactly one unramified extension  $L$  of  $K = \mathbb{Q}_p$  of degree  $n$  obtained by adjoining a primitive  $(p^n - 1)$ -th root of unity, say  $\theta$ . Moreover according to [9, Corollary 2], the extension  $L/K$  constitutes a cyclic extension such that  $\text{Gal}(L/K) = \langle \sigma \rangle$  where  $\sigma$  is defined by  $\sigma(\theta) = \theta^p$ . Since  $-1$  is not a square in  $K$  so  $p = 2^{\alpha}l - 1 \equiv 3 \pmod{4}$  by [4, Proposition 3.4.2] and thus  $\alpha \geq 2$ .

Let  $E_i := \{b \in L : \sigma^{\frac{n}{2^i}}(b) = -b\}$  where  $1 \leq i \leq \alpha - 1$ . The hypothesis  $\alpha \leq a + 1$  means that  $1 \leq i \leq a$ . Let  $w_i, \eta_i$  be as in Lemma 10. Again by Lemma 10,  $f_{b_i, \sigma}$  ( $b_i \in E_i$ ) is degenerate if and only if  $\eta_i$  is  $2^i$ -th root of unity such that  $\sigma(\eta_i) = -\eta_i^{-1}$ . As  $2^i \mid 2^{\alpha} \mid p + 1 \mid p^n - 1$ , this would mean that  $\langle \eta_i \rangle \leq \langle \theta \rangle$  and consequently,  $\sigma(\eta_i) = \eta_i^p$ . But then

$$\sigma(\eta_i)\eta_i = \eta_i^{p+1} = \eta_i^{2^{\alpha}l} = 1.$$

It follows that  $f_{b_i, \sigma}$  is non-degenerate. Hence  $\mathcal{E}_i$  is an  $n$ -subspace, where  $\mathcal{E}_i$  is the subspace of  $A^1$  corresponding to  $E_i$ .

Similarly let  $\mathcal{V}_j$  ( $1 \leq j \leq 2$ ) be the subspace of  $A^1$  corresponding to  $V_j$ . Then by Lemmas 11 and 5,  $\mathcal{V}_j$  is an  $(n - 2)$ -subspace. The theorem now follows.

**Remark 19.** In the situation of Theorem D for  $p = 2$  the decomposition (16) holds true in view of Remark 17. □

6. A 3-dimensional 4-subspace in  $\text{Alt}_4(\mathbb{Q})$

Let  $K := \mathbb{Q}$  and  $L$  be the cyclotomic field  $\mathbb{Q}(\eta)$  where  $\eta$  is a primitive 5-th root of unity in  $\mathbb{C}$ . Then  $L/K$  is a cyclic extension of degree 4. We will show that the maximum dimension of a 4-subspace inside  $A^1$  is 3. Let  $b = x + y\eta + z\eta^2 + w\eta^3 \in L$ , where  $x, y, z, w \in \mathbb{Q}$ . We take the automorphism  $\sigma$  defined by  $\sigma(\eta) = \eta^3$  as a generator of  $\text{Gal}(L/K)$ . Using the theory of Gauss periods we may find the basis, namely,  $\{1, \eta^2 + \eta^3\}$  for  $L_2/\mathbb{Q}$ . By Proposition 7,  $f_{b, \sigma}$  is degenerate if and only if  $N_{L/L_2}(b) \in \mathbb{Q}$ , that is, the coefficient of  $\eta^2 + \eta^3$  in  $N_{L/L_2}(b)$  is zero. It is straight-forward to check that this coefficient is  $-xy + xz + xw - yz + yw - zw$ . In this situation we thus obtain the following.

**Proposition 20.** *The maximum dimension of a 4-subspace inside  $A^1$  equals to a maximum dimension of a totally anisotropic subspace of  $L$  with respect to the following quadratic form*

$$\mathcal{Q}(x, y, z, w) = xy - xz - xw + yz - yw + zw.$$

**Proof.** Clear. □

**Theorem 21 (Legendre's Theorem ([7, Theorem 1, Chapter 5])).** *Suppose  $a, b, c \in \mathbb{Z}$  are such that  $abc$  is a non-zero square-free integer. Then the equation  $aX^2 + bY^2 + cZ^2 = 0$  has a non-trivial  $\mathbb{Z}$ -solution if and only if*

- (i)  $a, b, c$  do not all have the same sign;
- (iia)  $-bc$  is a square modulo  $|a|$ ,
- (iib)  $-ac$  is a square modulo  $|b|$  and
- (iic)  $-ab$  is a square modulo  $|c|$ .

**Theorem 22.** *The maximum dimension of a 4-subspace in  $A^1$  is 3.*

**Proof.** Let  $U$  be the  $\mathbb{Q}$ -subspace of  $L$  spanned by  $\{\eta + \eta^2, -1 + \eta^3, 1 + \eta\}$ . Let  $b = c_1(\eta + \eta^2) + c_2(-1 + \eta^3) + c_3(1 + \eta)$ . We claim that  $\mathcal{W} := \{f_{b, \sigma} : b \in U\} \leq A^1$  is the desired 4-subspace. Indeed, according to proposition 20 we need to show that the quadratic form

$$\mathcal{Q}(c_1, c_2, c_3) = c_1^2 + c_2^2 + c_3^2 + c_1c_3 - 3c_2c_3$$

has no non-trivial integer solution. It can be checked that  $\mathcal{Q}$  reduces to its diagonal form

$$\mathcal{Q}' = c_1^2 + c_2^2 - 6c_3^2.$$

To complete the proof, it suffices to show that  $\mathcal{Q}'$  has no non-trivial integer solutions. Based on Theorem 21 it is evident that  $\mathcal{Q}'$  has no non-trivial integer solutions since  $-ab = -1$  is not square modulo  $|c| = 6$ .  $\square$

## 7. Conclusion

Eigenspaces of the elements of the Galois group yield constant rank subspaces in  $\text{Alt}_K(L)$ . We can always find an  $n$ -subspace of dimension  $n/2$  in  $A^i$  for an arbitrary field  $K$  (Remark 14). However, this may not be the maximum possible dimension of an  $n$ -subspace in  $A^1$  (as is evident from the example in Section 5) unless  $n = 2k$  with  $k$  odd (Theorem A) or  $K$  is finite (or more generally  $C^1$  [5, Lemma 3]). Moreover unless  $K$  is finite it is not clear that we get an  $n$ -subspace of maximum dimension of  $\text{Alt}_n(K)$  in this way. The question of the maximum dimension of an  $n$ -subspace in  $\text{Alt}_n(K)$  is closely related to other invariants for skew-forms including  $d(K, n, 1)$  and  $s_n(K)$  defined in [1] and [5] respectively. In particular, it is unknown to the authors if there is a 6-subspace in  $\text{Alt}_6(\mathbb{Q})$  of dimension four.

## Declaration of Interest

The author do not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and have declared no affiliation other than their research organisations.

## References

- [1] J. Buhler, R. Gupta and J. Harris, "Isotropic subspaces for skewforms and maximal abelian subgroups of  $p$ -groups", *J. Algebra* **108** (1987), no. 1, pp. 269–279.
- [2] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory", *J. Comb. Theory, Ser. A* **25** (1978), no. 3, pp. 226–241.
- [3] P. Delsarte and J.-M. Goethals, "Alternating bilinear forms over  $GF(q)$ ", *J. Comb. Theory, Ser. A* **19** (1975), pp. 26–50.
- [4] F. Q. Gouvêa,  *$p$ -adic numbers. An introduction*, Springer, 1993, pp. vi+282.
- [5] R. Gow and R. Quinlan, "On the vanishing of subspaces of alternating bilinear forms", *Linear Multilinear Algebra* **54** (2006), no. 6, pp. 415–428.
- [6] R. Gow and R. Quinlan, "Galois extensions and subspaces of alternating bilinear forms with special rank properties", *Linear Algebra Appl.* **430** (2009), no. 8-9, pp. 2212–2224.
- [7] E. Grosswald, *Representations of integers as sums of squares*, Springer, 1985, pp. xi+251.
- [8] S. Lang, *Algebra.*, third edition, Addison-Wesley Publishing Group, 1993.
- [9] A. Weil, *Basic number theory*, Springer, 1995, pp. xviii+315.