國立台灣大學理學院數學系碩士論文

Department of Mathematics
National Taiwan University
Master Thesis

奇數維度特殊正交群的算術不變量理論

On Arithmetic Invariant Theory for Special Orthogonal Group of Odd Degree

陳健樺

Chien-Hua Chen

指導教授：陳其誠博士

Advisor: Ki-Seng Tan, Ph.D

中華民國 104 年 6 月

June, 2015

誌謝

首先我要感謝陳其誠老師這兩年的教導，每次在我讀書或讀論文遇到問題想很久想不出來去找老師的時候，老師常常會耐心的跟我討論。在討論的過程中，我常常學到一些自己原本不是很懂的事情或者能綜合老師的看法得到一些新的想法，這些想法往往是解決問題的關鍵。老師平常也會跟我們聊一些做人處事的道理，讓我覺得在這兩年不只是訓練我的數學能力，也在陶冶我的心靈。

我還要感謝在台大這兩年認識的人還有大學時期的朋友們。感謝天數 538 的柏傑、偉宏、冠中、俊德、仁傑，在我生活得很緊繃的時候會常常找我出去放鬆心情，修課或讀書上有問題的時候也會跟我一起討論。感謝我的室友柏誠，每次我很晚回家的時候還會跟我出門買宵夜，心情不好的時候也有人可以聊天。感謝大學的好朋友家揚，我們常常聊著著自己對於未來的規劃，讓我時時記得我的目標是什麼。感謝常常找我們聊天的江金倉老師，老師常常介紹我們台北好吃的東西，也會跟我們分享他的人生經歷，讓我也覺得學到不少東西。

最後，我要感謝我的父母。當初我決定讀數學的時候沒有阻止我，讓我無後顧之憂的專注在數學上。在碩士的這兩年裡，每當我遇到挫折的時候，爸媽也不斷鼓勵我堅持自己的理想，讓我能從挫折中站起來繼續面對其他挑戰。

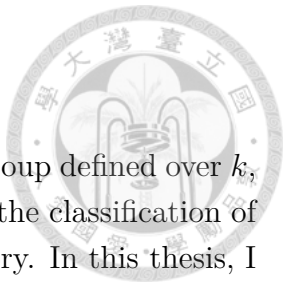
摘要

令 G 為一可簡約代數群、k 是一個特徵數為奇數的體、k^s 是 k 的分離封閉體，而 V 是 G 的一個表現。當我們考慮 $G(k^s)$ 作用在 $V(k^s)$ 上的軌跡的時候，幾何不變量理論給了我們一種分類這些軌跡的方法。然而當我們考慮 $G(k)$ 作用在 $V(k)$ 上的軌跡時，我們對於這個問題並沒有一個有系統的分類方法。在我的碩士論文裡，我研讀了 Bhargava 跟 Gross 的論文，他們針對奇數維度特殊正交群及它的一些表現發展了一套有系統的方法去分類這些特殊情況的軌跡。Bhargava 與 Gross 首先把分類軌跡的問題與伽羅瓦上同調理論做一個連結，而後利用這個連結去發展一些新的觀點及方法分類這些特殊情況的軌跡。

Abstract

Let G be a reductive group , k be a field of odd characteristic with a seperable closure k^s, and V be a representation of G. The geometric invariant theory deals with the classification of $G(k^s)$-orbits on V. In this thesis, I study the paper of Bhargava and Gross that deals with the problem on the classification of the $G(k)$-orbits on V which allows us to translate this problem into a language of Galois Cohomology. Then we deliver several approaches to solve this problem in some special cases.

Contents



1. Introduction

Let k be a field with a separable closure k^s, G be a reductive group defined over k, and V be a representation of G, also defined over k. In general, the classification of the $G(k^s)$-orbits on V is treated by the geometric invariant theory. In this thesis, I study the paper of Bhargava and Gross (cf. [Bhargava]) that deals with the problem on the classification of the $G(k)$-orbits on V. We refer this subject as the arithmetic invariant theory.

Let $\mathfrak{O}_k$ and $\mathfrak{O}_{k^s}$ denote respectively the sets of $G(k)$-orbits and $G(k^s)$-orbits on $V(k)$ and $V(k^s)$.

1.1. Relation between $\mathfrak{O}_k$ and $\mathfrak{O}_{k^s}$.

Let

$$\mathfrak{c} : \mathfrak{O}_k \longrightarrow \mathfrak{O}_{k^s}$$

be the natural (forgetful) map sending a k-orbit to its k^s-orbit. Let $\mathfrak{v} \in \mathfrak{O}_k$ and write $\mathfrak{c}(\mathfrak{v}) = \mathfrak{w}$. Our main aim is to classify the inverse image $\mathfrak{c}^{-1}(\mathfrak{w})$ for each $\mathfrak{v}$. We shall first relate this pre-image to some Galois cohomology. For simplicity, if A is a group with a continuous action of $\mathrm{Gal}(k^s/k)$ in the sense that the stabilizer of each $a \in A$ is an open subgroup, we denote the Galois cohomology $\mathrm{H}^1(\mathrm{Gal}(k^s/k), A)$ by $\mathrm{H}^1(k, A)$, and also $\mathrm{H}^q(\mathrm{Gal}(k^s/k), A)$ by $\mathrm{H}^q(k, A)$ for commutative A. Let v be a vector in $V(k)$ representing an orbit $\mathfrak{v} \in \mathfrak{O}_{k^s}$ and let $G_v \subset G$ denote its stabilizer. It is a closed subgroup of G and is defined over k.

Proposition 1.1.1. *Let notation be as above. There is a bijection between $\mathfrak{c}^{-1}(\mathfrak{w})$ and the kernel of the map*

$$\gamma : \mathrm{H}^1(k, G_v(k^s)) \to \mathrm{H}^1(k, G(k^s)).$$

Here the kernel of γ is defined to be the pre-image $\gamma^{-1}(0)$. Therefore, our task is to determine the kernel $\gamma^{-1}(0)$.

Proof. We have the exact sequence of $G(k^s)$-sets

$$1 \longrightarrow G_v(k^s) \longrightarrow G(k^s) \longrightarrow \mathfrak{w} \longrightarrow 1$$

that gives rise to the long exact sequence

$$\mathfrak{v} \to \mathfrak{w} \cap \mathfrak{O}_k \xrightarrow{\alpha} \mathrm{H}^1(k, G_v(k^s)) \xrightarrow{\gamma} \mathrm{H}^1(k, G(k^s))$$

and then the proposition is proved by interpreting $\mathfrak{w} \cap \mathfrak{O}_k$ as $\mathfrak{c}^{-1}(\mathfrak{w})$. Indeed, if $w \in \mathfrak{w} \cap \mathfrak{O}_k$ is a k-rational vector in the $G(k^s)$-orbit of v, then $w = g \cdot v$ for

some $g \in G(k^s)$ and such g is well-defined up to right multiplication by elements of $G_v(k^s)$. Now $\forall \sigma \in \mathrm{Gal}(k^s/k)$, we have $a(w)_\sigma := g^{-1} \cdot g^\sigma \in G_v(k^s)$ and the assignment $\sigma \mapsto a(w)_\sigma$ is a 1-cocycle $a(w)$ of $\mathrm{Gal}(k^s/k)$ with values in $G_v(k^s)$. Then we check that $a(w)$ is a coboundary if and only if $w \in \mathfrak{v}$ and also $a(w)$ and $a(w')$ differ by a coboundary if and only if w and w' are in the same $G(k)$-orbit. □

In this thesis, we try to determine the kernel of γ for the three cases where $G = \mathrm{SO}(W)$, W is an odd dimensional orthogonal space and $V = W$, $\Lambda^2(W)$ or $\mathrm{Sym}^2(W)$. The theory turns out very rich and interesting, too, with many aspects of arithmetic and geometry involved. The thesis is organized as follow. In §2, we recall the basic facts on odd dimensional orthogonal spaces and set the notation. In §3, we identify in each of the three cases the stabilizers G_v and establish the corresponding main theorems on γ. In §4, we discuss in the third case the relation of G_v and certain jacobian variety. In §5, we consider the cases of k being a finite field, a local field, or a global field. Finally, for the convenience of the readers, in the appendix we include a brief review of the Galois descent theory.

2. Setting

2.1. **Orthogonal space.** Let k be a field of $char(k) \neq 2$ and let W be an orthogonal space over k, by which we mean there is associated a non-degenerate bilinear from

$$<,>: W \times W \longrightarrow k.$$

Definition 2.1.1. *Let A be the corresponding matrix of the bilinear from with respect to a chosen basis so that $< w, w' >= w^t \cdot A \cdot w'$ for $w, w' \in W$. We define the determinant of W to be the residue class of* $\det A$ *modulo* $(k^*)^2$.

In the following, by abuse of language we shall simply say that the determinant of W is d to refer that it is actually d modulo $(k^*)^2$. As usually, by the bilinear from, we identify the dual space W^* with W by the isomorphism

$$W \xrightarrow{\sim} W^*, \quad w \mapsto w^* : w' \to < w', w > . \tag{1}$$

Let W' be another orthogonal space with the bilinear form $<,>'$ and let $T : W \to W'$ be a k-linear transformation. We define the adjoint transformation $T^* : W' \to W$ such that

$$< Tv, v' >' = < v, T^* v' >, \text{ for every } v \in W, v' \in W'.$$

If $\mathcal{B}$ and $\mathcal{B}'$ are bases of W and W'. Then for the associate matrices $[T]_{\mathcal{B},\mathcal{B}'}$ and $[T^*]_{\mathcal{B}',\mathcal{B}}$, we have

$$[T^*]_{\mathcal{B}',\mathcal{B}} = [T]^t_{\mathcal{B},\mathcal{B}'}$$

so these two matrices have the same determinant:

$$\det(T^*) = \det(T).$$

Two orthogonal space W and W' are isomorphic if there is a surjective orthogonal linear transformation $g : W \to W'$:

$$< gv, gw >' =< v, w >, \quad v, w \in W.$$

The condition is equivalent to

$$< v, g^*gw >=< g^*gv, w >=< v, w >, \quad \text{for all } \ v, w \in W.$$

Since $<,>$ is non-degenerate, such g is invertible with $g^{-1} = g^*$ and

$$\det(g) = \pm 1. \tag{2}$$

Lemma 2.1.2. *Two isomorphic orthogonal spaces have the same determinant.*

Proof. Let A and A' be the matrix of $<,>$ and $< \ . \ >'$ with respect to $\mathcal{B}$ and $\mathcal{B}'$. Then $[g]^t_{\mathcal{B},\mathcal{B}'} \cdot A' \cdot [g]_{\mathcal{B},\mathcal{B}'} = A$.

□

Definition 2.1.3. *An orthogonal space W of dimension $2n+1$, $n \geq 1$, is split if and only if there exists a subspace $U \subset W$ of dimension n such that $U \subset U^{\perp}$.*

From now on, we assume that W is a split orthogonal space of dimension $2n+1$, $n \geq 1$, with determinant $(-1)^n$.

The proof of the following lemma can be found in [SBF].

Lemma 2.1.4. *If W is a split orthogonal space of dimension $2n+1$, $n \geq 1$, with determinant $(-1)^n$, then there is an ordered basis*

$$\mathcal{B} = \{e_1, e_2, \cdots, e_n, u, f_1, f_2, \cdots, f_n\}$$

of W with inner product given by

$$< e_i, e_j >=< f_i, f_j >=< e_i, u >=< f_j, u >= 0,$$

$$< e_i, f_j >= \delta_{ij}.$$

$$< u, u >= 1.$$

We shall fix a basis described in the lemma and call it the *standard* basis.

2.2. **The special orthogonal group.**

Definition 2.2.1. *We define the orthogonal group*

$$\mathrm{O}(W) := \{g \in GL(W) : gg^* = g^*g = 1\}$$

and the special orthogonal group

$$\mathrm{SO}(W) := \{g \in GL(W) : gg^* = g^*g = 1, \det(g) = 1\}.$$

2.3. **Special representations of** $\mathrm{SO}(W)$**.** From now on denote $G = \mathrm{SO}(W)$. We shall consider three representations V of G over k and define the associated discriminate function:

$$\triangle : V(k^s) \longrightarrow k^s.$$

In the first case, $V = W$ with the natural action of G and

$$\triangle(v) =< v, v >, \text{ for } v \in V.$$

For the second and the third representation, we first take the identification:

$$W \otimes W = W \otimes W^* = \mathrm{Hom}(W, W), \tag{3}$$

where the first identification is via (1) and the second is by taking

$$w \otimes w^*(v) = w^*(v) \cdot w, \text{ for all } w \in W.$$

Let G acts on $W \otimes W$ by $g(w_1 \otimes w_2) = gw_1 \otimes gw_2$, and via (3) for $T \in \mathrm{Hom}(W, W)$,

$$g \cdot T = gTg^{-1}.$$

For such T, define

$$\triangle(T) := \mathrm{disc}(\det(xI - T)),$$

the discriminant of the characteristic polynomial of T. Recall that a polynomial has nonzero discriminant if and only if it's separable.

Consider the decomposition:

$$W \otimes W = \Lambda^2(W) \oplus \mathrm{Sym}^2(W)$$

and let the second and the third representation be the restriction of the action of G to $\Lambda^2(W)$ and $\mathrm{Sym}^2(W)$. Also, let the discriminant function to the restriction of the above to these subspaces. Therefore, in the second case,

$$V = \Lambda^2(W) = \{T : W \to W : T = -T^*\},$$

which is of dimension $2n^2+n$; while in the third case,

$$V = \mathrm{Sym}^2(W) = \{T : W \to W : T = T^*\},$$

which is of dimension $2n^2+3n+1$.

2.4. **A conventional use of notation.** We shall follow the convention that if L is a k-algebra of finite rank then L^* also denote the algebraic group having the same defining equation as L^*. Namely, if $\{e_1, ., e_n\}$ is a basis of L over k as vector space and $e_i \cdot e_j = \sum_h a_{i,j,h} e_h$, $a_{i,j,h} \in k$, under the multiplication in L and the identity element $1 = \sum_i \alpha_i e_i$, then L^* is the algebraic variety with the coordinate ring $k[x_1, ..., x_n, y_1, ..., y_n]$ subject to the condition

$$\sum_h \sum_{i.j} a_{i,j,h} x_i y_j e_h \left(= \sum_i x_i e_i \cdot \sum_j y_i e_j = 1 \right) = \sum_h \alpha_h e_h.$$

Thus, in such notation, if l is a commutative k-algebra, then the set of l-points:

$$L^*(l) = (l \otimes_k L)^*.$$

If N is a subgroup of $L*$ defined by equalities of polynomials, then N also denotes the corresponding closed subgroup of L^*.

3. Main theorems

Let V denote one of the three representation of G introduced in §2.3. In this chapter, for each $v \in V(k)$ with discriminant $\triangle(v) \neq 0$, our aim is to determine G_v, $\mathrm{H}^1(k, G_v)$ and the kernel of γ. Recall that $\mathcal{B} = \{e_1, e_2, \cdots, e_n, u, f_1, f_2, \cdots, f_n\}$ is chosen to be the standard basis of W.

3.1. **The case $V = W$.** For each $d \in k^*$, denote $v_d := e_1 + (1/2)d \cdot f_1$ whose discriminant $\triangle(v) = d$.

Lemma 3.1.1. *Two vectors $v, w \in V(k)$ are in the same orbit of G, if and only if $\triangle(v) = \triangle(w)$.*

Proof. If $v, w \in V(k)$ are in the same orbit of G, then $\triangle(v) = \triangle(w)$. The other direction of the proof basically follows from Witt's extension theorem which says that if (V_1, Q) and (V_2, Q') are isometric non-degenerate quadratic spaces, then every injective linear map $s_0 : U \to V_2$ of a subspace U of V_1 such that $Q' \circ s_0 = Q$ can be extended to a linear isomorphism $s : V_1 \to V_2$ such that $Q' \circ s = Q$ (cf. Theorem 11.15 in [ALA]). We may assume that $\triangle(w) = d$ and $v = v_d$. Let Q denote the

bilinear form $<,>$. Since $Q(v,v) = Q(w,w)$, the injective linear map $kv \to V$ defined by mapping v to w extends an isometry

$$s : (V,Q) \to (V,Q).$$

Let $t : V \to V$ be the linear map such that $t(e_1) = -e_1$, $t(e_j) - e_j$, $j \neq 1$, $t(u) = u$, $t(f_1) = -f_1$, $t(f_j) - f_j$, $j \neq 1$, and set $s' = (-s) \circ t$. Then $s(v) = s'(w)$ and $\det(s') = -\det(s)$. Thus, one of s and s' belongs to G and v and w are in the same G-orbit..

□

Lemma 3.1.2. *Let $v \in V(k)$ be such that $\triangle(v) \neq 0$ and $U := (kv)^{\perp}$. Then the restriction $g \mapsto g\,|_U$ gives rise to an isomorphism $G_v \to \mathrm{SO}(U)$.*

Proof. Since $\triangle(v) \neq 0$, $v \notin U$ and $W = kv \oplus U$ as orthogonal space. Every element in $\mathrm{SO}(U)$ can be extended in an obvious way to a unique orthogonal transformation on W. □

Note that in the above lemma U is actually an orthogonal space of dimension $2n$, since the restriction of $<,>$ to U is non-degenerate, and its determinant equals $(-1)^n \triangle(v)$.

Lemma 3.1.3. *Every $2n$-dimensional orthogonal subspace of W of determinant $(-1)^n d \neq 0$ is isomorphic to $(kv_d)^{\perp}$.*

Proof. If U is a $2n$-dimensional orthogonal subspace of W of determinant $(-1)^n d$, then its orthogonal compliment $U^{\perp}$ can be expressed as kv with $\triangle(v) = d$. Lemma 3.1.1 says kv is isomorphic to kv_d and we have

$$U \oplus kv = (kv_d)^{\perp} \oplus (kv_d).$$

Then the lemma follows from the Witt's cancelation theorem below. □

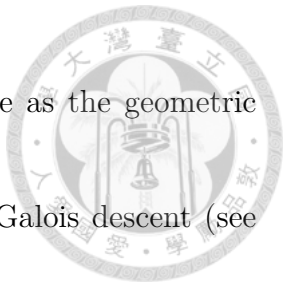
Lemma 3.1.4 (Witt's cancelation theorem)**.** *If $W = W_1 \oplus W_2$ and $W' = W_1' \oplus W_2'$ and $W \simeq W'$ and $W_1 \simeq W_1'$, as orthogonal spaces, then $W_2 \simeq W_2'$.*

Proof. See Theorem 11.16 in [ALA] □

Theorem 1. *If $V = W$ and $v \in V(k)$ is such that $\triangle(v) \neq 0$, then the map*

$$\gamma : H^1(k, G_v) \to H^1(k, G)$$

is injective.



Thus in this case the arithmetic invariant theory is the same as the geometric invariant theory.

Proof. Denote $d := \triangle(v)$. By Lemma 3.1.3 and the theory of Galois descent (see §6), we may identify $H^1(k, G)$ with

$$E_W(k^s/k) := \left\{ \begin{array}{c} k\text{-isomorphism classes of } 2n+1\text{-dimensional orthogonal} \\ \text{spaces } W' \text{ of determinant } (-1)^n \end{array} \right\}$$

and $H^1(k, G_v)$ with

$$E_U =: \left\{ \begin{array}{c} k\text{-isomorphism classes of } 2n\text{-dimensional orthogonal} \\ \text{spaces } U' \text{ of determinant } (-1)^n d \end{array} \right\}.$$

Now in the commutative diagram

$$\begin{array}{ccc} H^1(k, \mathrm{SO}(U)) & \xrightarrow{\gamma} & H^1(k, \mathrm{SO}(W)) \\ \| & & \| \\ E_U(k^s/k) & \longrightarrow & E_W(k^s/k), \end{array}$$

the lower right-arrow sends each $U' \in E_U(k^s/k)$ to $W' := U' \oplus kv$ in $E_W(k^s/k)$ and the "identity elements" of both $H^1(k, \mathrm{SO}(U))$ and $H^1(k, \mathrm{SO}(W))$ are identified with U and W, respectively. Hence the theorem follows from the Witt's cancelation theorem again.

□

3.2. **The $V = \Lambda^2(W)$ case.** Recall that every element T of $V = \Lambda^2(W)$ is viewed as a skew self-adjoint operator on W. In this case, the characteristic polynomial is an odd function, and hence we can write

$$f(x) := \det(xI - T) = x^{2n+1} + c_2 x^{2n-1} + c_4 x^{2n-3} + \cdots + c_2 x = x g(x^2).$$

Thus, $\triangle(T) \neq 0$ if and only if f is separable.

3.2.1. *the special operator.*

Lemma 3.2.1. *If T is a skew self-adjoint operator on W with $\triangle(T) \neq 0$, then the characteristic polynomial $\det(xI - T)$ is separable, of the form $xg(x^2)$. Conversely, for each monic separable polynomial $f(x) = xg(x^2)$, of degree $2n+1$, there is a skew self-adjoint operators $T : W \to W$ such that $\det(xI - T) = f(x)$.*

For a separable polynomial $f(x) = xg(x^2)$, denote $L = k[x]/(f(x))$, which is an étale algebras of rank $2n+1$. By Chinese Remainder Theorem,

$$L = E \oplus k,$$

where $E = k[x]/(g(x^2))$. Let $K = k[y]/(g(y))$. Then $y \mapsto x^2$ induce an inclusion of K into E. Also, $x \mapsto -x$ induces an involution τ on E and L with fixed algebras K and $K \bigoplus k$ respectively. Over k^s, $f(x)$ splits completely into the product

$$x\prod_{i=1}^{n}(x-a_i)(x+a_i).$$

Write $E_0 = k^s[x]/(x)$, $E_i^{\pm} := k^s[x]/(x \pm a_i) \cong k^s$, $1 \le i \le n$. Then

$$k^s \otimes_k L = E_1^+ \times E_1^- \times \cdots \times E_n^+ \times E_n^- \times E_0. \tag{4}$$

We can extend k^s-linearly τ to an involution on $k^s \otimes_k L$. In view of (4), we have

$$(x_1^+, x_1^-, ..., x_0)^\tau = (x_1^-, x_1^+, ..., x_0). \tag{5}$$

Proof. It remains to prove the second assertion of the lemma. Let $\beta \in L$ denote the residue class of x. Then $f(\beta) = 0$, $f'(\beta) \in L^*$, $\beta^\tau = -\beta$, and $L = k + k\beta + k\beta^2 + \cdots + k\beta^{2n}$. Define the bilinear form $<,>$ on L by setting

$$< \lambda, \mu >:= \text{the coefficient of } \beta^{2n} \text{ in the product } (-1)^n\lambda\mu^\tau.$$

We can represent $<,>$ as a matrix A with respect to the basis $\{1, \beta, \cdots, \beta^{2n}\}$. Thus

$$A = \begin{pmatrix} & & & (-1)^n \\ & & \iddots & * \\ & (-1)^{3n-1} & * & * \\ (-1)^{3n} & * & * & * \end{pmatrix}$$

and $\det(A) = (\prod_{j=0}^{2n}(-1)^{n+j})(-1)^{n+1} = (-1)^n$, which means $<,>$ is non-degenerate of determinant $(-1)^n$. The n-dimensional subspace $L^0 := k + k\beta + k\beta^2 + \cdots + k\beta^{n-1}$ satisfies $L^0 \subset (L^0)^\perp$. Hence, L is a split orthogonal space and by Lemma 2.1.4, there is an isometry $\theta : L \to W$ over k which is unique up to composition with orthogonal transformations of W. Consider the skew self-adjoint operator $t : L \to L$ defined by $t(\lambda) = \beta\lambda$. The characteristic polynomial of t equals to $f(x)$. Thus $T = \theta t\theta^{-1} : W \to W$ is a skew self-adjoint operator with characteristic polynomial equal to $f(x)$. □

3.2.2. *The stabilizer.* For the rest of this section, *let T denote the specific skew self-adjoint operator corresponding to t in the above proof.* Note that the $G(k)$-orbit of T is independent of the choice of θ. If $\theta' = \lambda \circ \theta$ for some $\lambda \in \mathrm{O}(W)(k)$, then one of λ and $-\lambda$ is contained in $\mathrm{SO}(W)$, it sends T to $\theta' t \theta'^{-1}$ as the action of G is by conjugation.

Since f is separable, T is semi-simple, and hence the centralizer of T in $\mathrm{End}_k(W)$ is just $k[T]$, which can be identified with $k[x]/(f(x)) = L$ by identifying T with x modulo $f(x)$. Similarly, if l is a field extension of k, then the centralizer of T in $\mathrm{End}_l(W)$ is $l \otimes_k L$. Therefore, in the notation of §2.4, under the conjugate action of $\mathrm{GL}(W)$, the stabilizer of T is isomorphic to L^*. Note that for $\lambda \in k[T]$ its determinant as an operator on W is the same as the determinant of the k-linear map $L \to L$, $z \mapsto \lambda \cdot z$. By (4), if $\lambda = (\lambda_1^+, \lambda_1^-, ..., \lambda_n^+, \lambda_n^-, \lambda_0)$, then

$$\det(\lambda) = \lambda_1^+ \lambda_1^- \cdot \cdots \cdot \lambda_n^+ \cdot \lambda_n^- \cdot \lambda_0. \tag{6}$$

Lemma 3.2.2. *In $G = \mathrm{SO}(W)$, the stabilizer*

$$G_T = \{\lambda \in L^* : \lambda^{1+\tau} = 1, \det(\lambda) = 1\},$$

which is a maximal torus of G.

Proof. By the definition of $<,>$, an element $\lambda \in L^*$ is contained in $\mathrm{O}(W)$ if and only if $\lambda \cdot \lambda^\tau = 1$. This proves the first part of the lemma.

By (5) and (6), $\lambda \in G_T$ if and only if

$$\lambda_i^+ \lambda_i^- = 1, \quad i = 1, ..., n, \quad \text{and} \quad \lambda_0 = 1. \tag{7}$$

This implies G_T is a torus. That it is a maximal torus follows from the fact that the stabilizer of every element in the adjoint representation of the compact Lie group $\mathrm{SO}(W)$ contains a maximal torus (cf. [TASM]). □

Recall that if X is a scheme over K, then the Weil restriction of scalar $\mathrm{Res}_{K/k}X$ is the scheme such that for every k algebra F,

$$\mathrm{Res}_{K/k}X(F) = X(F \otimes_k K).$$

In particular, if $X = \mathrm{Spec}B$ the spectrum of a K-algebra $B = K[x_1, ..., x_\mu]/(f_1, ..., f_\nu)$ and $v_1, ..., v_n$ is a k- basis of K, then $\mathrm{Res}_{K/k}X = \mathrm{Spec}B'$ where $B' = k[x_{ij}]/(f_{ih})$, $i = 1, ..., n$, $j = 1, ..., \mu$, $h = 1, ..., \nu$, such that if we write $x_j = \sum_{i=1}^n x_{ij} v_i$, then $f_h = \sum_{i=1}^n f_{ih} v_i$.

Let $U_1(E/K)$ denote the algebraic group over K given by

$$\{\alpha \in E^* : \alpha^{1+\tau} = 1\}$$

in the convention of §2.4. Then by (7), the k-algebraic group G_T is nothing but the Weil restriction of scalar of $U_1(E/K)$.

Lemma 3.2.3. *We have* $G_T \cong \mathrm{Res}_{K/k} U_1(E/K)$.

3.2.3. *The k^s-orbit of T.* Let $f(x) = xg(x^2)$ be a separable polynomial of degree $2n$ and let T be the special operator associated to $f(x)$.

Lemma 3.2.4. *Every skew self-adjoint operator S having characteristic polynomial equal to $f(x)$ is in the $G(k^s)$-orbit of T, and vice versa.*

Proof. Since f(x) is separable, it is the minimal polynomial of T and S. Therefore, T and S are similar by some element $u \in \mathrm{GL}(W)(k^s)$ in the sense that $S = uTu^{-1}$. Now the equalities

$$(uTu^{-1})^* = S^* = -S = -(uTu^{-1})$$

and

$$(uTu^{-1})^* = (u^{-1})^* T^* u^* = (u^{-1})^*(-T)u^*$$

imply

$$u^* u T = T u^* u.$$

Therefore, as explained in §3.2.2, $u^*u \in L^*(k^s)$, and since it is self-adjoint, it is actually contained in $K^* \times k^*$. By (5), the norm homomorphism $L^*(k^s) \to K^*(k^s) \times (k^s)^*$, $h \mapsto h^{1+\tau}$ is surjective. Hence we can write $u^*u = h^{1+\tau}$. Consider the operator $uh^{-1} \in \mathrm{GL}(W)(k^s)$, it is orthogonal:

$$(uh^{-1})^* = (h^{-1})^* u^* = h^{-\tau} u^* = h(u^*u)^{-1} u^* = hu^{-1} = (uh^{-1})^{-1}.$$

Choose $u_0 = \pm uh^{-1}$ to have $\det u^0 = 1$. Then $u_0 \in \mathrm{SO}(k^s)$. Since $h \in L^*$, $hTh^{-1} = T$, and hence u_0 sends T to S:

$$u_0 T u_0^{-1} = uh^{-1} T h u^{-1} = uTu^{-1} = S.$$

The second assertion is obvious. □

Corollary 3.2.5. *If S is skew self-adjoint operator having $\triangle(S) \neq 0$, then G_S is a maximal torus of G.*

Suppose in the above lemma S is k-rational. Let u_0 be as in the above proof so that $u_0 \in G(k^s)$. For each $\sigma \in \mathrm{Gal}(k^s/k)$, $u_0 = u_0^\sigma \xi_\sigma$, for some $\xi_\sigma \in G_T(k^s)$. Then $\sigma \mapsto \xi_\sigma$ defines a $G_T(k^s)$-valued 1-cocycle of $\mathrm{Gal}(k^s/k)$ and its class in $\mathrm{H}^1(k, G_T)$ is exact the element of $\ker \gamma$ corresponding to S (see Proposition 1.1.1 and its proof).

3.2.4. *k-orbits.* Now we give a more precise description of $\ker \gamma$ other than the above one. For each k-rational element $\kappa \in K^*$, denote $\alpha := \alpha_\kappa := (\kappa, 1) \in K^* \times k^*$ and let W_κ denote the orthogonal space with the same underlying linear space as L, while its symmetric bilinear form $<,>_\kappa$ defined by

$$< \lambda, \mu >_\kappa := \text{the coefficient of } \beta^{2n} \text{ in the product } (-1)^n \alpha \lambda \mu^\tau.$$

Thus W_κ is an orthogonal space of dimension $2n+1$ and determent $(-1)^n$, because $< \lambda, \mu >_\kappa = < \alpha \cdot \lambda, \mu >$ and by (6), $\det \alpha \in (k^*)^2$. Let $N : E^* \to K^*$ be the norm map sending ξ to $\xi^{1+\tau}$. If $\kappa' = \kappa \cdot h^{1+\tau}$, h a k-rational element of E^*, then the linear map $L \to L$, $z \mapsto hz$ gives rise to an orthogonal isomorphism $W_\kappa \to W_{\kappa'}$. By descent theory, $\mathrm{H}^1(k, \mathrm{SO}(W))$ is nothing but the set of the isomorphism classes of orthogonal spaces of determinant $(-1)^n$. Thus, the above discussion gives rise to

$$\gamma' : K^*/NE^* \to \mathrm{H}^1(k, \mathrm{SO}(W))$$

that maps the residue class of κ to the isomorphic class of W_κ.

Theorem 2. *Let $V = \Lambda^2(W)$ and let T be the specific skew self-adjoint operator of V described in* §3.2.2 *so that its characteristic polynomial $f(x) := xg(x^2)$ is separable. Then the $\mathrm{SO}(k^s)$-orbit of T is formed by all skew self-adjoint operators S with characteristic polynomial equal to $f(x)$. Furthermore, the cohomology group $\mathrm{H}^1(k, G_T)$ can be identified with the quotient K^*/NE^*, where $K = k[y]/(g(y))$, $E = k[x]/(g(x^2))$ and $N : E^* \to K^*$ is the group homomorphism induced by $x \mapsto -y^2$, and the map γ in* proposition 1.1.1 *can be identified with γ' defined above.*

Proof. Apply Lemma 3.2.3 and consider the exact sequence of $\mathrm{Gal}(k^s/k)$-modules

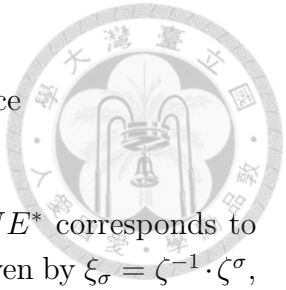
$$1 \to G_T(k^s) \to \mathrm{Res}_{E/k}\mathbb{G}_m(k^s) \xrightarrow{N} \mathrm{Res}_{K/k}\mathbb{G}_m(k^s) \to 1$$

which is the same as

$$1 \to G_T(k^s) \to (k^s \otimes_k E)^* \xrightarrow{N} (k^s \otimes_k K)^* \to 1.$$

It induces the long exact sequence

$$1 \to G_T(k) \to E^* \xrightarrow{N} K^* \xrightarrow{\delta} \mathrm{H}^1(k, G_T(k^s)) \to \mathrm{H}^1(k, (E \otimes_k k^s)^*) \tag{8}$$



By (4) and Hilbert Theorem 90, $\mathrm{H}^1(k, (E \otimes_k k^s)^*) = 0$, and hence

$$\mathrm{H}^1(k, G_T(k^s)) \cong K^*/NE^*.$$

Under this isomorphism, the residue class of $\kappa \in K^*$ modulo NE^* corresponds to the cohomology class of the 1-cocycle $\xi : \mathrm{Gal}(k^s/k) \to G_T(k^s)$ given by $\xi_\sigma = \zeta^{-1} \cdot \zeta^\sigma$, for each $\sigma \in \mathrm{Gal}(k^s/k)$, where $\zeta \in E^*(k^s)$ satisfying $N(\zeta) = \kappa$. We need to show that the descent theory also associates W_κ to the cohomology class of ξ.

Recall that W_κ is the orthogonal space with the same underlying space as L but with $<,>_\kappa$ as its symmetric bi-linear form. Write

$$\zeta_1 = (\zeta, 1) \in E(k^s)^* \times (k^s)* = L^*(k^s).$$

Then the map $u \mapsto \zeta_1 \cdot u$ gives rise to an orthogonal isomorphism $\phi_{\zeta_1} : W_\kappa \to L$, and the descent theory also associates W_κ to the cohomology class represented by the 1-cocycle η with

$$\eta_\sigma = (\phi_{\zeta_1})^{-1} \circ \phi_{\zeta_1}^\sigma = (\zeta_1)^{-1} \cdot \zeta_1^\sigma = \zeta^{-1} \cdot \zeta^\sigma = \xi_\sigma.$$

.

□

3.3. **The $V = \mathrm{Sym}^2(W)$ case.** In this case, we show that G_T is a finite commutative group scheme of order 2^{2n} over k and we also give an explicit description of the map $\gamma : \mathrm{H}^1(k, G_T) \to \mathrm{H}^1(k, G)$ for specific T.

3.3.1. *The specific T.*

Lemma 3.3.1. *If T is a self-adjoint operator on W with $\triangle(T) \neq 0$, then the characteristic polynomial $\det(xI - T)$ is separable of degree $2n + 1$. Conversely, for each monic separable polynomial $f(x)$ of degree $2n + 1$, there is a self-adjoint operators $T : W \to W$ such that $\det(xI - T) = f(x)$.*

In this section (§3.3), for a monic separable polynomial $f(x)$, let $L = k[x]/(f(x))$ and let β be the residue class of x in L. Let $\tau : L \to L$ be the automorphism mapping β to $-\beta$.

Proof. Define on L the symmetric bilinear form $<,>$ by

$$< \lambda, \mu >:= \text{the coefficient of } \beta^{2n} \text{ in the product } \lambda\mu.$$

This endows L the structure of a split orthogonal space of determinant $(-1)^n$. Let $\theta : L \to W$ be an orthogonal isomorphism (by Lemma 2.1.4) over k and let t

denote the linear map such that $t(\lambda) = \beta\lambda$. Then t is self-adjoint of characteristic polynomial $f(x)$, and hence so is the operator $T = \theta t \theta^{-1}$ on W. □

Note that here the choice of θ doesn't affect the $G(k)$-orbit on T. For the rest of this section, *let T denote the specific self-adjoint operator corresponding to t in the above proof.*

3.3.2. *The stabilizer.* Similar to the previous case, since f is separable, T is semi-simple, and hence the centralizer of T in $\mathrm{End}_k(W)$ is just $k[T]$, which can be identified with $k[x]/(f(x)) = L$ by identifying T with x modulo $f(x)$. Under this identification, if $S \in L$, then $S^* = S$. Hence,

$$G_T := \{\lambda \in L^* \mid \ \lambda^2 = 1, \det(\lambda) = 1\}.$$

Let $N : L^* \to k^*$ denote the norm map that send each $y \in L^*$ to $\det(y)$ and we extend it to a morphism

$$N : \mathrm{Res}_{L/k}\mathbb{G}_m \to \mathbb{G}_m$$

and by restrict it to $\mathrm{Res}_{L/k}\mu_2$ we get the exact sequence

$$1 \to (\mathrm{Res}_{L/k}\mu_2)_{N=1} \to \mathrm{Res}_{L/k}(\mu_2) \xrightarrow{N} \mu_2 \to 1. \tag{9}$$

Here $(\mathrm{Res}_{L/k}\mu_2)_{N=1}$ is defined to be the kernel of the map $N : \mathrm{Res}_{L/k}\mu_2 \to \mu_2$. Then we check directly that for each commutative k-algebra F,

$$G_T(F) = \{\lambda \in (L \otimes_k F)^* : \lambda^2 = 1, \det_F(\lambda) = 1\} = (Res_{L/k}\mu_2)_{N=1}(F)$$

and actually $G_T = (\mathrm{Res}_{L/k}\mu_2)_{N=1}$.

Lemma 3.3.2. *In $G = \mathrm{SO}(W)$, the stabilizer $G_T = (\mathrm{Res}_{L/k}\mu_2)_{N=1}$ which is a finite étale group scheme of order 2^{2n}.*

Proof. Since the characteristic of k is not 2, μ_2 is an étale group scheme of order 2. Therefore, $\mathrm{Res}_{L/k}(\mu_2) \times_{\mathrm{Spec}k} \mathrm{Spec}L = (\mu_2)^{2n+1}$ is an étale group scheme of order 2^{2n+1} over L. Thus, if $\mathrm{Res}_{L/k}(\mu_2) = \mathrm{Spec}A$, then $A \otimes_k L$ is separable over L. Since L is separable over k, A must be separable over k, and hence $\mathrm{Res}_{L/k}(\mu_2)$ is étale over k . The rest of the lemma follows from (9). □

3.3.3. *The k^s-orbit of T.*

Lemma 3.3.3. *Every self-adjoint operator S having characteristic polynomial equal to $f(x)$ is in the $G(k^s)$-orbit of T, and vice versa.*

Proof. Since f(x) is separable, T and S are similar by some element $g \in \mathrm{GL}(W)$. Now $(gTg^{-1})^* = (gTg^{-1})$ and $(gTg^{-1})^* = (g^{-1})^*T^*g^* = (g^{-1})^*Tg^*$ implies $g^*gT = Tg^*g$, and hence $g^*g \in L^*$. Let $h \in (L \otimes_k k^s)^*$ such that $g^*g = h^2$. Choose $u_0 = \pm gh^{-1}$ to have $u_0 \in \mathrm{SO}(W)(k^s)$. We have $u_0Tu_0^{-1} = S$. □

Corollary 3.3.4. *In $\mathrm{SO}(W)$, the stabilizer of every self-adjoint operator S having separable characteristic polynomial $f(x)$ is a finite étale group scheme of order 2^{2n}.*

3.3.4. *The k-orbit.* The norm homomorphism $N : L^* \to k^*$ induces the homomorphism $L^*/L^{*2} \to k^*/k^{*2}$ whose kernel we denote by $(L^*/L^{*2})_{N=1}$. Let $\alpha \in L^*$ be such that $N(\alpha) \in k^{*2}$. Define the orthogonal space W_α whose underlying vector space is L, while the symmetric bilinear form $<,>$ is given by

$$< \lambda, \mu >_\alpha := \text{the coefficient of } \beta^{2n} \text{ in the product } \alpha\lambda\mu.$$

The space W_α is a $2n+1$ dimensional orthogonal space over k with determinant $(-1)^n$, because $< \lambda, \mu >_\alpha = < \alpha \cdot \lambda, \mu >$ and $\det \alpha = N(\alpha) \in (k^*)^2$. If $\alpha' = \lambda^2\alpha$, for some $\lambda \in L^*$, then $\mu \mapsto \lambda\mu$ gives rise to an isomorphism between $W_{\alpha'}$ and W_α as orthogonal spaces. Therefore, we can associate to each element $[\alpha] \in (L^*/L^{*2})_{N=1}$ the k-isomorphic class $[W_\alpha]$ of W_α. By descent theory, this defines the map

$$\gamma' : (L^*/L^{*2})_{N=1} \to \mathrm{H}^1(k, \mathrm{SO}(W)). \tag{10}$$

Theorem 3. *Let $V = \mathrm{Sym}^2(W)$ and let T be the specific self-adjoint operator of V described in* §3.3.1 *so that its characteristic polynomial $f(x)$ is separable. Then the $\mathrm{SO}(k^s)$-orbit of T is formed by all self-adjoint operators S with characteristic polynomial equal to $f(x)$. Furthermore, the cohomology group $\mathrm{H}^1(k, G_T)$ can be identified with the quotient $(L^*/L^{*2})_{N=1}$, where $L = k[x]/(f(x))$ and $N : L^* \to k^*$ is the norm map, and the map γ in* proposition 1.1.1 *can be identified with γ' in* (10).

Proof. The exact sequence (9) induces the long exact sequence

$$\cdots \to \mu_2(L) \xrightarrow{N} \{\pm 1\} \xrightarrow{\delta} \mathrm{H}^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1}) \to \mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2) \xrightarrow{N_*} \mathrm{H}^1(k, \mu_2) \to \cdots .$$

Since $N(-1) = -1$, the map $\mu_2(L) \xrightarrow{N} \{\pm 1\}$ is surjective. Then we identify the group $\mathrm{H}^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1})$ with $(L^*/L^{*2})_{N=1}$ via the commutative diagram

$$\begin{array}{ccccc} 0 \longrightarrow \mathrm{H}^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1}) & \to & \mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2) & \xrightarrow{N_*} & H^1(k, \mu_2) \\ & & \| & & \| \\ 0 \longrightarrow (L^*/L^{*2})_{N=1} & \longrightarrow & L^*/L^{*2} & \longrightarrow & k^*/k^{*2}, \end{array}$$

where the two equalities are by Kummer theory. Under this identification, if $\alpha \in L^*$, $N(\alpha) \in k^{*2}$ represents the class $[\alpha] \in (L^*/L^{*2})_{N=1}$ and $h \in (L \otimes k^s)^*$, $h^2 = \alpha$, then $[\alpha]$ corresponds to the class $[\rho] \in \mathrm{H}^1(k, (\mathrm{Res}_{L/k}\mu_2)_{N=1})$ represented by the cocycle ρ such that $\rho_\sigma = h^\sigma/h \in \mu_2(L \otimes k^s)^*_{N=1}$. Here $\mu_2(L \otimes k^s)^*_{N=1}$ denotes the kernel of $\mu_2(L \otimes k^s) \xrightarrow{N} \{\pm 1\}$. For such α and h, the map sending λ to $h\lambda$ is an orthogonal isomorphism from W_α to L. By descent theory, $\gamma'([\alpha])$ is also represented by the cocycle ρ.

□

4. more discussion on the representation V=$\mathrm{Sym}^2(W)$

In the second and the third case, we have known that for each $\alpha \in \mathrm{H}^1(k, G_T)$, the class $\gamma(\alpha)$ is represented by the orthogonal space W_α such that $\alpha \in \ker \gamma$ if and only if W_α is split (Definition 2.1.3). In this section, we construct in the third case some non-trivial $\alpha \neq 1$ such that W_α is split.

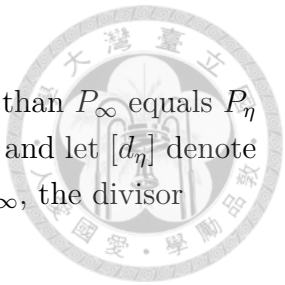
Let C be the smooth projective hyper elliptic curve of genus n over k with affine equation $y^2 = f(x)$ where $f(x)$ is given as in Theorem 3. Let J be the Jacobian of C over k.

4.1. **The group scheme** $J[2]$**.**

Lemma 4.1.1. *The group scheme $J[2]$ of 2-torsion points on the Jacobian of C is a finite étale group schemes over k of order 2^{2n}.*

Because $char(k) \neq 2$, this is well known (cf. [ABV]). As before, write $L = k[x]/(f(x)) = k + k\beta + \cdots + k\beta^{2n}$, where$f(\beta) = 0$. Let $\pi : C \to \mathbb{P}^1$ be the two-to-one covering sending $P := [x : y : z]$ (in projective coordinate) to $x_P := [x : z]$. Let $P_\infty = [0 : 1 : 0]$ be the k-rational Weierstrass point above $[1 : 0]$ (the infinite point on $\mathbb{P}^1$).

Each root α of $f(x)$ in k^s corresponds to a unique non-trivial k-algebra homomorphism $\eta : L \to k^s$ so that $\alpha = \eta(\beta)$. For such η, denote $P_\eta = [\eta(\beta) : 0 : 1]$, which is a



Weierstrass point on C, and every Weierstrass point on C other than P_∞ equals P_η for a unique η. Let d_η denote the divisor $P_\eta - P_\infty$ of degree zero and let $[d_\eta]$ denote its divisor class. Since π is ramified of index 2 at each P_η and P_∞, the divisor

$$\operatorname{div}(y) = \sum_{\text{all } \eta} d_\eta. \tag{11}$$

Since the divisor of the rational function $x - \eta(\beta)$ on $\mathbb{P}^1$ equals $[\eta(\beta) : 1] - [1 : 0]$, on C the divisor

$$\operatorname{div}(\pi^*(x - \eta(\beta)) = 2P_\eta - 2P_\infty = 2d_\eta$$

(cf. [AEC, Proposition 2.6]). Hence $[d_\eta] \in J[2](k^s)$.

Lemma 4.1.2. *The group $J[2](k^s)$ is generated by all $[d_\eta]$ associated to k-algebra homomorphisms $\eta : L \to k^s$, subject to the condition*

$$\sum_{all\ \eta} [d_\eta] = 0.$$

Proof. The condition is due to (11). Since $J[2](k^s)$ is a $\mathbb{F}_2$-vector space, it is sufficient to show that if $m \leq 2n$, then

$$\sum_{i=1}^{m} [d_{\eta_i}] \neq 0.$$

If this were not true, then we would have

$$\sum_{i=1}^{m} d_{\eta_i} = \operatorname{div}(z)$$

for some $z \in k^s(C)$, the field of k^s-rational function on C. Then z has only pole at P_∞ of order m. Let V be the k^s-space of rational function on C with only pole at P_∞ of order at most $2n$. Riemann-Roch theorem says that V has dimension equal to $1-n+2n+1 = n+1$, because C is of genus n. Since $1, x, \cdots, x^n$ are all in V and are linearly independent over k^s, they form a basis of V. Because $z \in V$, it must be a linear combination of $1, x, \cdots, x^n$. However, since the order of a polynomial of x at every Weierstress point is even while the order of z at each Weierstress point P_{η_i} is 1, we have a contradiction. □

Let T be the special operator on W associated to f.

Lemma 4.1.3. *The group scheme $J[2]$ of 2-torsion points on the Jacobian of C is isomorphic to the stabilizer G_T of T in $\mathrm{SO}(W)$.*

Proof. The category of commutative finite étale group schemes over k is equivalent to the category of finite $G(k^s/k)$-modules (cf. [AGS, §6.4]). Thus, we need to show that $J[2](k^s) \cong (\mathrm{Res}_{L/k}(\mu_2)(k^s))_{N=1}$ as $G(k^s/k)$-modules.

By Chinese Remainder Theorem,

$$L \otimes_k k^s = \underbrace{k^s \times k^s \times \cdots \times k^s}_{2n+1},$$

and if $pr_i : L \otimes_k k^s \to k^s$ is the projection onto the ith factor, then the composition

$$\eta_i : L \xrightarrow{\iota} L \otimes_k k^s \xrightarrow{pr_i} k^s,$$

where ι denotes the natural map $u \mapsto u \otimes 1$, is a non-trivial k-algebra homomorphism, and vice versa. In particular, since every for $\sigma \in \mathrm{Gal}(k^s/k)$, the composition

$$\sigma \circ \eta_i : L \to k^s$$

is also a non-trivial k-algebra homomorphism, there is a unique $j =: i^\sigma$ such that

$$\sigma \circ \eta_i = \eta_{i^\sigma}. \tag{12}$$

The $\mathrm{Gal}(k^s/k)$-module structure of $L \otimes_k k^s$ is given by the action of $\mathrm{Gal}(k^s/k)$ on the right factor k^s. Write t_i for $pr_i(t)$ for $t \in L \otimes_k k^s$. Then we have

$$(t^\sigma)_{i^\sigma} = (t_i)^\sigma. \tag{13}$$

Now,

$$\mathrm{Res}_{L/k}(\mu_2)(k^s) = \mu_2(L \otimes_k k^s) = \underbrace{\mu_2(k^s) \times \mu_2(k^s) \times \cdots \times \mu_2(k^s)}_{2n+1},$$

where each $\mu(k^s) = \{\pm 1\}$ and by (13), the action of σ just send the ith factor to the i^σth. In particular, the diagonal map

$$\{\pm 1\} \xrightarrow{\Delta} \{\pm 1\} \times \cdots \times \{\pm 1\}$$

identifies $\mu_2(k^s)$ as a $\mathrm{Gal}(k^s/k)$ submodule of $\mathrm{Res}_{L/k}\mu_2(k^s)$. Moreover, since $2n+1$ is an odd integer, the restriction of the norm map $\Delta(\mu(k^s)) \xrightarrow{N} \mu_2(k^s)$ is an isomorphism. Therefore, the exact sequence of $\mathrm{Gal}(k^s/k)$-modules

$$0 \to (\mathrm{Res}_{L/k}\mu_2(k^s))_{N=1} \to \mathrm{Res}_{L/k}\mu_2(k^s) \to \mu_2(k^s) \to 0$$

actually splits. Hence

$$(\mathrm{Res}_{L/k}(\mu_2)(k^s))_{N=1} \cong \mathrm{Res}_{L/k}\mu_2(k^s)/\mu_2(k^s).$$

Let A denote the $2n+1$ dimension $\mathbb{F}_2$-vector space with η_i, $i = 1, ..., 2n+1$, as basis and let $\mathrm{Gal}(k^s/k)$ acts on A by (12). Then the map $A \to \mathrm{Res}_{L/k}\mu_2(k^s)$ sending $\sum_i a_i\eta_i$ to $((-1)^{a_1}, (-1)^{a_2}, ..., (-1)^{a_{2n+1}})$ is an isomorphism of $\mathrm{Gal}(k^s/k)$-modules. Then we complete the proof by noting that the $\mathbb{F}_2$-homomorphism mapping η_i to $[d_{\eta_i}]$ identifies $J[2](k^s)$ with $A/\mathbb{F}_2$ which is isomorphic to $\mathrm{Res}_{L/k}\mu_2(k^s)/\mu_2(k^s)$.

□

4.2. **Special classes in** $\ker\gamma$**.** The exact sequence of Galois modules

$$0 \to J[2](k^s) \to J(k^s) \xrightarrow{2} J(k^s) \to 0$$

induces the exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{H}^1(k, J[2]) \to \mathrm{H}^1(k, J)[2] \to 0 \tag{14}$$

By the lemma above we have $\mathrm{H}^1(k, J[2]) \cong \mathrm{H}^1(k, G_T)$.

Proposition 4.2.1. *The subgroup $J(k)/2J(k)$ of $H^1(k, J[2]) = H^1(k, G_T)$ lies in* $\ker\gamma$.

Proof. Recall that in §3.3.4, we associate to each class $\alpha \in \mathrm{H}^1(k, G_T)$ the orthogonal space W_α whose underlying space is L, with symmetric bilinear form

$$< \lambda, \mu >_\alpha := \text{the coefficient of } \beta^{2n} \text{ in the product } \alpha\lambda\mu.$$

Now we use "left multiplication by β" to construct another symmetric bilinear form $< \beta\lambda, \mu >_\alpha$ on L. Let $M = L \bigoplus k$, a $2n+2$-dimensional vector space over k. We define two bi-linear forms (or quadratic forms) on M: for $(\lambda, a) \in M$,

$$Q(\lambda, a) = < \lambda, \lambda >_\alpha,$$
$$Q'(\lambda, a) = < \beta\lambda, \lambda >_\alpha + a^2.$$

The pencil $uQ - vQ'$ with $u, v \in k^s$ has discriminant $v^{2n+2}f(u/v)$. Indeed, write l_β for the matrix associated to the left multiplication by β, and $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ and

$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} l_\beta & 0 \\ 0 & 1 \end{pmatrix}$ for those associate to Q and Q', respectively. Then

$$\begin{aligned} \operatorname{disc}(uQ - vQ') &= \det(u \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} - v \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} l_\beta & 0 \\ 0 & 1 \end{pmatrix}) \\ &= \det \begin{pmatrix} uA - vAl_\beta & 0 \\ 0 & -v \end{pmatrix} \\ &= (-v) \det(A) \det((u/v \cdot I - l_\beta)v) \\ &= (-v)(-1)^{2n+1} v^{2n+1} f(u/v) \\ &= v^{2n+2} f(u/v). \end{aligned}$$

Thus, the pencil $uQ - vQ'$ is non-degenerate and contains exactly $2n + 2$ singular elements over k^s, which are the quadric Q, and the $2n + 1$ quadrics $\eta(\beta)Q - Q'$ with $f(\eta(\beta)) = 0$. There is a Fano variety F_α whose k^s-points corresponds to n-dimensional k^s-subspaces Z of M which are isotropic for all of the quadrics in the pencil, and F_α is actually a principle homogeneous space of order 2 of the Jacobian J, corresponding to the image of α in $\mathrm{H}^1(k, J)[2]$ [Donagi].

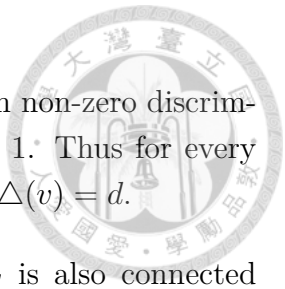
If $\alpha \in J(k)/2J(k)$, then by (14), the image of α in $\mathrm{H}^1(k, J)[2]$ is trivial, so that the corresponding principle homogeneous space F_α has a k-rational point. Thus, there is a n-dimensional subspace Z of M over k which is isotropic for all quadrics in the pencil, hence isotropic for Q and Q'. Since Z is isotropic for Q', Z contains no elements in M of the form $(0, a)$, $a \neq 0$. Hence, the projection of Z onto L is a n-dimensional k-subspace of L which is isotropic for Q. This implies the symmetric bilinear form $<, >_\alpha$ is split. Therefore, α is in the kernel of γ.

□

5. Arithmetic fields

In this section, we consider the special cases where k is a finite field, a local field, or a global field. As before, the cases where $V = W$, $V = \Lambda^2(W)$ and $V = \mathrm{Sym}^2(W)$ are respectively referred as the first, send and third case.

5.1. **The finite field case.** Let k be a finite field of odd order q. By Lang's theorem (cf. [GC, III §2.3 Theorem 1′]), $\mathrm{H}^1(k, \mathrm{SO}(W)) = 1$ since $\mathrm{SO}(W)$ is connected. Thus by Galois descent theory, every orthogonal space of dimension $2n + 1$ with determinant $(-1)^n$ is split so that $\mathrm{H}^1(k, G_T) \subseteq \ker \gamma$.



5.1.1. *The first case.* In the notation of §3.1, for each $v \in V$ with non-zero discriminant, $G_v = \mathrm{SO}(U)$ which is also connected, hence $\mathrm{H}^1(k, G_v) = 1$. Thus for every non-zero element $d \in k^*$, there is a unique orbit of vectors with $\triangle(v) = d$.

5.1.2. *The second case.* For each $S \in V$ with $\triangle(S) \neq 0$, G_S is also connected because it is a maximal torus (Corollary 3.2.5) of the connected algebraic group $\mathrm{SO}(W)$, hence has trivial cohomology. Thus for any separable polynomial $f(x) = xg(x^2)$, there is a unique orbit of $S \in V$ with characteristic polynomial $f(x)$.

5.1.3. *The third case.* Let $T \in V$ be the special operator with non-zero discriminant so that $G_T = (\mathrm{Res}_{L/k}\mu_2)_{N=1}$. The exact sequence (9) induces the long exact sequence

$$\begin{array}{ccccccc} \cdots \to \mu_2(L) \xrightarrow{N} \mu_2(k) & \to \mathrm{H}^1(k, G_T) & \to \mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2) & \xrightarrow{N_*} \mathrm{H}^1(k, \mu_2) \to \cdots \\ & \| & \| & \\ & (L^*/L^{*2}) & \xrightarrow{N_*} (k^*/k^{*2}). & \end{array} \tag{15}$$

Let $m+1$ denotes the number of irreducible factors of $f(x) \in k[x]$. Then

$$|\mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2)| = 2^{m+1}.$$

Also, since $2n+1$ is an odd integer, the composition $\mu_2(k) \to \mu_2(L) \xrightarrow{N} \mu_2(k)$ is surjective. Hence $\mathrm{H}^1(k, G_T) \to \mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2)$ is injective. The lemma below asserts that

$$\mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2) \xrightarrow{N_*} \mathrm{H}^1(k, \mu_2)$$

is actually surjective. These together imply

$$|\mathrm{H}^1(k, G_T)| = 2^m = |(\mu_2(L))_{N=1}| = |G_T(k)|.$$

This means that there are 2^m distinct $G(k)$-orbits with characteristic polynomial $f(x)$ that lie in the $G(k^s)$-orbit with characteristic polynomial $f(x)$. Since the order of each orbit equals to

$$\frac{|\mathrm{SO}(W)(k)|}{|G_T(k)|} = \frac{|\mathrm{SO}(W)(k)|}{2^m},$$

the number of self-adjoint operators $S \in V$ associated to a fixed separable polynomial equals to $|\mathrm{SO}(W)(k)|$.

Lemma 5.1.1. *The map* $\mathrm{H}^1(k, \mathrm{Res}_{L/k}\mu_2) \xrightarrow{N_*} \mathrm{H}^1(k, \mu_2)$ *is surjective.*

Proof. By (15), it is sufficient to show that $L^* \xrightarrow{N} k^*$ is surjective. By Chinese Remainder Theorem, we can write $L^* = \prod_{i=1}^{m+1} L_i^*$, where each L_i is a field extension of k, so that if $t = (t_1, ..., t_{m+1}) \in L^*$, then $N(t) = \prod_{i=1}^{m+1} N_{L_i/k}(t_i)$. Since k is a finite field, each norm map $N_{L_i/k}$ is surjective. Hence the lemma follows. □

By Lang's theorem, $\mathrm{H}^1(k, J) = 0$,where J is the Jacobian of the smooth hyperelliptic curve $y^2 = f(x)$ of genus n over k. Hence $J(k)/2J(k) \cong \mathrm{H}^1(k, G_T)$ and every orbit associated to $f(x)$ comes from a k-rational point on the Jacobian.

5.2. **The non-archimedean local field case.** Let k be a non-archimedean local field, with ring of integer $\mathcal{O}$ and finite residue field $\mathbb{F} := \mathcal{O}/\pi\mathcal{O}$ of odd order p^α.

The simply-connected covering of SO is the spin group spin. We have an exact sequence

$$1 \to \mu_2 \to \mathrm{spin} \to SO \to 1.$$

By Kneser's theorem (cf. [GC, III §3.1 Conjecture II(a)]) we have

$$\mathrm{H}^1(\mathrm{k}, \mathrm{spin(W)}) = 1,$$

and hence the injective connecting map:

$$\delta : \mathrm{H}^1(\mathrm{k}, \mathrm{SO(W)}) \hookrightarrow \mathrm{H}^2(\mathrm{k}, \mu_2) \cong \mathbb{Z}/2\mathbb{Z}.$$

5.2.1. *Surjectivity of δ.* We'll prove the surjectivity of δ by using induction on dimension of W.

Lemma 5.2.1. *Let V be a k-orthogonal space with $dim(V) = 2$, then $|H^1(k, SO(V)| = 1$ if $\det(V) = -1(mod\ k^{*2})$ and $|H^1(k, SO(V))| = 2$ if $\det(V) = -d \neq -1(mod\ k^{*2})$.*

Proof. (1) When $\det(V) = -1(mod\ k^{*2})$:

For every 2-dimensional orthogonal space $(V', < \cdot, \cdot >')$ with $\det(V') = -1(mod\ k^{*2})$, the case V' has a nonzero isotropic vector is clearly split.

We may assume V' contains no nonzero isotropic vectors. By using Gram-Schmidt's orthogonal process, there is an orthogonal basis $\mathcal{B} = \{e_1, e_2\}$ such that

$$[< \cdot, \cdot >]_{\mathcal{B}} = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}, \text{where } c_1c_2 = -l^2 \text{ for some } l \in k^*.$$

Consider $v_1 := (l)e_1 + c_1e_2$, we have $< v_1, v_1 >= 0$. Thus $(V', < \cdot, \cdot >)$ is split.

(2) When $\det(V) = -d \neq -1(mod\ k^{*2})$:

For every 2-dimensional orthogonal space $(V', <\cdot,\cdot>')$ with $\det(V') \neq -1(mod\ k^{*2})$, V' contains no nonzero isotropic vectors. By using Gram-schmidt's process , there is an orthogonal basis $\mathcal{B} = \{e_1, e_2\}$ and the quadratic form q associates to $<\cdot,\cdot>$ under this basis is of the form

$$q(xe_1 + ye_2) = ax^2 - by^2 \quad \text{where } xe_1 + ye_2 \in V' \text{ and } ab = d.$$

Consider the special case $a = 1,\ b = d$. This gives an orthogonal space $(V_0, <\cdot,\cdot>_0)$, and the associated quadratic form q_0 is just the norm N from $k(\sqrt{d})$ to k.
On the other hand, $|k^*/Nk(\sqrt{d})| = 2$ by local class field theory, so we choose $c \in k^*$ not a norm from $k(\sqrt{d})$, consider the orthogonal space
$(V_1, <\cdot,\cdot>_1)$ with associated quadratic form q_1 of the form $cx^2 - cdy^2$. Then V_0 and V_1 have the same determinant but they are not isomorphic because q_0 and q_1 represent different numbers in k. Hence $|H^1(k, SO(V))| = 2$.

□

Lemma 5.2.2. *Let $(V, <\cdot,\cdot>)$ be a k-orthogonal space with $dim(V) = 3$, then $|H^1(k, SO(V)| = 2$.*

Proof. If there is an isotropic vector v in V. Then the quadratic form q, which corresponds to $<\cdot,\cdot>$, represents zero. Hence q represents every number. This means that $\triangle(u) =< u, u >$ can be every number as u varies in V. If $\det(V) = a(mod\ k^{*2})$, we choose v such that $\triangle(v) \neq -a(mod\ k^{*2})$ and consider $V' = (kv)^{\perp}$. We have $det(V') \neq -1(mod\ k^{*2})$, thus $H^1(k, SO(V'))$ has 2 elements by Lemma5.2.1, and so is $H^1(k, SO(V))$.

If V contains no nonzero isotropic vector , then $(kv)^{\perp}$ also contains no isotropic vector, for every $v \in V$, and hence $H^1(k, SO(V'))$ has 2 elements by Lemma5.2.1, and so is $H^1(k, SO(V))$. □

Proposition 5.2.3. *Let $(V, <\cdot,\cdot>)$ be a k-orthogonal space with $dim(V) \geqslant 3$, then $|H^1(k, SO(V)| = 2$. This proves the surjectivity of δ.*

Proof. We prove by induction on $dim(V)$. When $dim(V) = 3$, the proposition holds by Lemma 5.2.2. Assume the proposition holds for $dim(V) = l$, we consider the case $dim(V) = l + 1$. By Choosing a vector $v \in V$, we have the decomposition $V = V' \oplus kv$ where $V' = (kv)^{\perp}$.

Now $V' \hookrightarrow V$ induces $H^1(k, SO(V')) \hookrightarrow H^1(k, SO(V))$(the proof is similar to Theorem 1), and the induction hypothesis asserts that $|H^1(k, SO(V'))| = 2$. Thus $|H^1(k, SO(V)| = 2$. □

5.2.2. *The first case.* By Lemma 5.2.1, $\mathrm{H}^1(k, G_v) = \mathrm{H}^1(k, \mathrm{SO}(U)) \cong \mathbb{Z}/2\mathbb{Z}$ except when $dim(W) = 3$ and $\triangle(v) = 1(mod\ k^{*2})$. Thus γ is bijection except in the special case.

5.2.3. *The second case.* Kottwitz has shown that γ is actually a group homomorphism when we identify $H^1(k, G_v)$ and $H^1(k, SO(W))$ as K^*/NE^* and $\mathbb{Z}/2\mathbb{Z}$ respectively. (cf. [Kottwiz]). Let $f(x) = xg(x^2)$,$K = k[x]/(g(x))$ and $E = k[x]/(g(x^2))$. By local class field theory, $|K^*/NE^*| = 2^m$ where m is the number of irreducible factors $g_i(x)$ of $g(x)$ such that $g_i(x^2)$ still irreducible over k. Kottwitz also shows that γ is surjective when $m \geqslant 1$. Thus when $m = 0$, the number of orbits with characteristic polynomial $f(x)$ is 1. And when $m \geqslant 1$, the number of such orbits is 2^{m-1}.

5.2.4. *The third case.* We can view $\mathrm{H}^1(k, J[2])$ as a $\mathbb{F}_2$-vector space. Let q denote the composition:

$$\mathrm{H}^1(k, G_v) = \mathrm{H}^1(k, J[2]) \underset{\gamma}{\to} \mathrm{H}^1(k, \mathrm{SO}(W)) \underset{\rho}{\xrightarrow{\sim}} \mathrm{H}^2(k, \mu_2)$$

and consider the bilinear map

$$\phi : H^1(k, J[2]) \times H^1(k, J[2]) \to H^2(k, \mu_2)$$

induced from the Weil pairing $e_2 : J[2] \times J[2] \to \mu_2$ by using cup product. Then q is actually a quadratic refinement of ϕ [Wang, theorem 2.15] in the sense that

$$\phi(a, b) = q(a + b) - q(a) - q(b) + q(0), \quad \text{for all a, b} \in \mathrm{H}^1(k, J[2]).$$

This implies ϕ is an even bilinear form, because for all $a \in \mathrm{H}^1(k, J[2])$

$$\phi(a, a) = q(a + a) - q(a) - q(a) + q(0) = q(2a) - 2q(a) + q(0) = 2q(0) = 0.$$

Moreover, q is a quadratic form since

$$q(0) = 0 \text{ and } q(cv) = c^2 q(v) \text{ for all } c \in \mathbb{F}_2\ ,\ v \in \mathrm{H}^1(\mathrm{k}, \mathrm{J}[2]).$$

Let $m + 1$ be the number of irreducible factors of $f(x)$ in $k[x]$. Then

$$L^* = \prod_{i=1}^{m+1} K_i*$$

where each K_i is a field extension of k. By Theorem 3

$$\mathrm{H^1(k, G_v) = (L^*/L^{*2})_{N=1} = (\prod_{i=1}^{m+1} K_i^*/K_i^{*2})_{N=1}}.$$

Each K_i is a local field of odd residue characteristic p. Hence, $|K_i^*/K_i^{*2}| = 2^2$ and $|(\prod_{i=1}^{m+1} K_i^*/K_i^{*2})_{N=1}| = 2^{2m}$. Therefore, which implies $\dim_{\mathbb{F}_2} \mathrm{H^1(k, J[2])} = 2m$. Moreover, the Arf invariant of the quadratic form q is 0 because there is a m dimensional $\mathbb{F}_2$-subspace $J(k)/2J(k)$ which is isotropic under q (Proposition 4.2.1). Therefore, the cardinality of $\ker(\gamma)$ equals $2^{m-1}(2^m + 1)$ (cf. [GALA, Theorem 6.2.38]) that, by Theorem 3, is the same as the number of orbits with characteristic polynomial equal to $f(x)$.

5.3. **The $k = \mathbb{R}$ case.**

We begin by recalling the definition of the signature of a non-degenerate real inner product space over $\mathbb{R}$. Given a non-degenerate real inner product (non-degenerate symmetric $\mathbb{R}$-bilinear map) space $(V, <, >)$, we can choose a suitable basis under which the $<, >$ correspond to the diagonal matrix D whose diagonal entries are ± 1.

Definition 5.3.1. *We say $(V, <, >)$ has signature (p, q) if there are p many 1's and q many -1's in the diagonal entries of D.*

Thus, two real inner product spaces having the same signature are isomorphic as orthogonal spaces. In the second and third case,$\mathrm{H^1(\mathbb{R}, G_T)}$ isomorphic to K^*/NE^* and $(L^*/L^{*2})_{N=1}$ respectively, both are elementary abelian 2-group. Here we only consider the case where $\mathrm{H^1(k, G_T)}$ has maximal rank.

5.3.1. *The first case.* Recall that $\mathrm{H^1(\mathbb{R}, SO(W))}$ represents the set of k-isomorphism classes of non-degenerate orthogonal spaces W' of dimension $2n+1$ and determinant $(-1)^n \in \mathbb{R}^*/\mathbb{R}^{*2}$. Since $\mathbb{R}^*/\mathbb{R}^{*2} = \{\pm 1\}$,

$$\mathrm{|H^1(k, SO(W))| = n + 1}$$

because the signature associated to each class must satisfy

$$p + q = 2n + 1 \quad \text{and} \quad q \equiv n \pmod 2.$$

Now $\mathrm{H^1(\mathbb{R}, G_v)} = \mathrm{H^1(\mathbb{R}, SO(U))}$ represents the set of $\mathbb{R}$-isomorphism classes of non-degenerate orthogonal spaces U' of dimension $2n$ and discriminant $\triangle(v)$ over $\mathbb{R}$. Because $\triangle(v) = \pm 1$, we separate our computation of $\mathrm{|H^1(\mathbb{R}, G_v)|}$ into two cases:

(1) $\triangle(v) = (-1)^n$:

This forces U' to have positive determinant so that its signature (p, q) satisfies

$$p + q = 2n \quad \text{and} \quad q \equiv 2 \pmod 2.$$

Hence $|\mathrm{H}^1(\mathbb{R}, \mathrm{G_v})| = \mathrm{n} + 1$.

(2) $\triangle(v) = (-1)^{n+1}$:

Then U' has negative determinant and its signature (p, q) satisfies

$$p + q = 2n \quad \text{and} \quad q \equiv 1 \pmod 2.$$

Hence $|\mathrm{H}^1(\mathbb{R}, \mathrm{G_v})| = \mathrm{n}$.

Therefore, γ is bijective when $\triangle(v) = (-1)^n$ and injective when $\triangle(v) = (-1)^{n+1}$.

5.3.2. *The second case.* To have K^*/NE^* achieve the maximal rank, we need to have $f(x) = x\prod_{i=1}^{n}(x^2 + c_i)$ where $c_i \in \mathbb{R}_{>0}$. Then

$$K^*/NE^* \cong (\mathbb{R}^*/\mathbb{R}_{>0})^n \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

The real orthogonal space W then decompose into n orthogonal T-invariant planes and an orthogonal line kv' with $Tv' = 0$. Indeed, by the strict real version of spectrum theorem, if S is a skew self adjoint operator on W, there is an orthogonal basis $\mathcal{A}$ of W such that

$$[S]_{\mathcal{A}} = \begin{pmatrix} M_1 & & O \\ & \ddots & \\ O & & M_l \end{pmatrix}$$

where $M_0 = 0$ and $M_i = \begin{pmatrix} 0 & -\sqrt{c_i}_i \\ \sqrt{c_i} & 0 \end{pmatrix}$, for $i = 1, ..., n$. If the orthogonal basis $\mathcal{A} = \{v_0, v_{11}, v_{12}, \cdots, v_{n1}, v_{n2}\}$, then

$$W = W_0 \oplus W_1 \oplus \cdots \oplus W_n$$

where $W_0 = \mathrm{span}\{v_0\}$, $W_i = \mathrm{span}\{v_{i1}, v_{i2}\}$ for $1 \leqslant i \leqslant n$, and

$$W_0 = \ker S \text{ and } Sv_{i1} = \sqrt{c_i}v_{i2}\ ,\ Sv_{i2} = -\sqrt{c_i}v_{i1}.$$

We regard this decomposition as the spectral decomposition of S.

Note that for each i,

$$< v_{i2}, v_{i2} >=< \frac{1}{\sqrt{c_i}}Sv_{i1}, \frac{1}{\sqrt{c_i}}Sv_{i1} >= \frac{1}{c_i} < v_{i1}, -S^2v_{i1} >=< v_{i1}, v_{i1} >,$$

and

$$< v_{i1}, v_{i2} >= \frac{1}{\sqrt{c_i}} < v_{i1}, Sv_{i1} >= \frac{1}{\sqrt{c_i}} < -Sv_{i1}, S_{i1} >= - < v_{i2}, v_{i1} >,$$

and hence $< v_{i1}, v_{i2} >= 0$, because $<,>$ is symmetric. Therefore, the signature of each W_i is either $(2,0)$ or $(0,2)$. Let the ordered set

$$\omega(S) := \{\omega(W_0), \omega(W_1), ..., \omega(W_n)\}$$

denote the signatures of W_0, W_1,...,W_n and call it the signature of S.

By using the standard basis $\mathcal{B}$, we see that the signature of W is $(n+1, n)$. Let m denote the positive integer such that $n = 2m+1$ or $n = 2m$. If n is odd, then W_0 has signature $(1,0)$ ad there are exactly m W_i having signature $(0,2)$; if n is even, then W_0 has signature $(0,1)$ and there are exactly m W_i having signature $(2,0)$.

Lemma 5.3.2. *Suppose $S, S' \in \Lambda^2(W)$ have the same characteristic polynomial $f(x) = x\prod_{i=1}^{n}(x^2 + c_i)$. Then S and S' lie in the same* $\mathrm{SO(W)}(\mathbb{R})$*-orbit if and only if they have the same signature.*

Proof. For each $g \in \mathrm{SO(W)}(\mathbb{R})$ the spectral decomposition of $S' := gSg^{-1}$ is

$$W = W_0' \oplus W_1' \oplus \cdots \oplus W_n'$$

where $W_0' = \mathrm{span}\{gv_0\}$, $W_i' = \mathrm{span}\{gv_{i1}, gv_{i2}\}$ for $1 \leqslant i \leqslant n$. Then since

$$< gu, gv >=< u, v >, \quad \text{for all } \ u, v \in \mathcal{B},$$

we have

$$\omega(S) := \omega(S').$$

Conversely , if $S, S' \in \Lambda^2(W)$ have the same signature and

$$W = W_0' \oplus W_1' \oplus \cdots \oplus W_n'$$

is the special decomposition of S', then because $\omega(W_j') = \omega(W_j)$, for $j = 0, ..., n$, we can arrange to have the corresponding basis

$$\mathcal{A}' = \{v_0', v_{11}', v_{12}', \cdots, v_{n1}', v_{n2}'\}$$

satisfying

$$< v_0, v_0 >=< v_0', v_0' >, \ < v_{i1}, v_{i1} >=< v_{i1}', v_{i1}' > \ \text{ and } \ < v_{i2}, v_{i2} >=< v_{i2}', v_{i2}' > .$$

Choose the linear map g such $gv_0 = \pm v_0'$, $gv_{i1} = v_{i1}'$ and $gv_{i2} = v_{i2}'$, $1 \leq i \leq n$ to have $g \in \mathrm{SO}(W)$. Then $S' = gSg^{-1}$. Hence S and S' are in the same $\mathrm{SO}(W)(\mathbb{R})$-orbit. □

Proposition 5.3.3. *Let m denote the positive integer such that $n = 2m+1$ or $n = 2m$. There are exactly $\binom{n}{m}$ elements in* $\ker\gamma$.

Proof. Let $S = T$. For every σ in the symmetric group S_n, let $g_{i,\sigma(i)} : W_i \to W_{\sigma(i)}$ be the isomorphism sending v_{i1}, v_{i2} respectively to $v_{\sigma(i)1}$, $v_{\sigma(i)2}$ and let

T^σ denote the linear transformation such that

$$T^\sigma \mid_{W_0} = T \mid_{W_0} \quad \text{and} \quad T^\sigma \mid_{W_i} = g_{i\sigma(i)}^{-1} \circ T \mid_{W_{\sigma(i)}} \circ g_{i\sigma(i)}.$$

Then $T^\sigma \in \Lambda^2(W)$. The above lemma says each $\mathrm{SO}(W)(\mathbb{R})$-orbit in $\ker\gamma$ contains at least one such T^σ and there are exactly $\binom{n}{m}$ $\mathrm{SO}(W)(\mathbb{R})$-orbit among

$$\{T^\sigma \mid \sigma \in S_n\}.$$

□

5.3.3. *The third case.* The 2-group $\mathrm{H}^1(\mathbb{R}, G_T)$ has maximal rank if and only if $f(x)$ factors completely over $\mathbb{R}$, say $f(x) = \prod_{i=1}^{2n+1}(x - c_i)$. In this case,

$$\mathrm{H}^1(\mathbb{R}, G_T) \cong (L^*/L^{*2})_{N=1} \cong ((R^*)^{2n+1}/(\mathbb{R}_{>0})^{2n+1})_{N=1} \cong (\mathbb{Z}/2\mathbb{Z})^{2n}.$$

tBy spectrum theorem, S is a self-adjoint operator on W of characteristic polynomial $f(x)$ if and only if there is an orthogonal basis $\mathcal{A} = \{v_1, v_2, \cdots, v_{2n+1},\}$ of W such that

$$[S]_{\mathcal{A}} = \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_{2n+1} \end{pmatrix}.$$

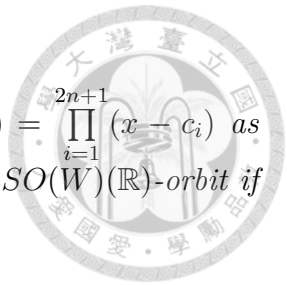
Accordingly,

$$W = W_1 \oplus W_2 \oplus \cdots \oplus W_{2n+1}$$

where $W_i = \mathrm{span}\{v_i\}$ and $Sv_i = c_i v_i$ for $1 \leqslant i \leqslant 2n+1$. Call this the special decomposition of S. We define the signature of S to be the ordered set

$$\omega(S) := \{\omega(W_1), ..., \omega(W_{2n+1})\}$$

where $\omega(W_i)$ denote the signature of W_i.



Lemma 5.3.4. *Let S, S' be elements of $\mathrm{Sym}^2(W)$ having $f(x) = \prod_{i=1}^{2n+1}(x - c_i)$ as their characteristic polynomial. Then S and S' lie in the same $SO(W)(\mathbb{R})$-orbit if and only if $\omega(S) = \omega(S')$.*

Proof. If $g \in \mathrm{SO}(W)(\mathbb{R})$, then the decomposition of gSg^{-1} is

$$W = W_1' \oplus \cdots \oplus W_{2n+1}'$$

where $W_i' = \mathrm{span}\{gv_i\}$ and $gSg^{-1}(gv_i) = gv_i$ for all i. Hence

$$< v_i, v_i >=< gv_i, gv_i > \quad \text{for all } 1 \leqslant i \leqslant 2n+1.$$

Conversely , if $S, S' \in \mathrm{Sym}^2(W)$ have the same signature and

$$W = W_1' \oplus W_1' \oplus \cdots \oplus W_{2n+1}'$$

is the special decomposition of S', then because $\omega(W_j') = \omega(W_j)$, for $j = 1, ..., 2n+1$, we can arrange to have the corresponding basis $\mathcal{A}' = \{v_1', \cdots, v_{2n+1}'\}$ such that

$$< v_i, v_i >=< v_i', v_i' > \text{ for all } 1 \leqslant i \leqslant 2n+1.$$

Choose a linear operator g such that $gv_1 = \pm v_1'$ and $gv_i = v_i'$, for $j = 2, ..., 2n+1$, to have $g \in \mathrm{SO}(W)(\mathbb{R})$. Then $S = gSg^{-1}$. □

The proof of the following is similar to that of Proposition 5.3.3.

Proposition 5.3.5. *There are $\binom{2n+1}{n}$ elements in $\ker\gamma$.*

5.4. **The Global field case.** Here we only consider the case $V = \mathrm{Sym}^2(W)$.

The exact sequence

$$0 \to J[2] \xrightarrow{\iota} J \xrightarrow{2} J \to 0$$

induces the commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J(k)/2J(k) & \longrightarrow & \mathrm{H}^1(k, J[2]) & \xrightarrow{\iota_*} & \mathrm{H}^1(k, J)[2] & \longrightarrow & 0 \\ & & \downarrow a & & \downarrow b & & \downarrow c & & \\ 0 & \longrightarrow & \prod_v J(k_v)/2J(k_v) & \xrightarrow{\delta} & \prod_v \mathrm{H}^1(k_v, J[2]) & \xrightarrow{\iota_*} & \prod_v \mathrm{H}^1(k_v, J)[2] & \longrightarrow & 0 \end{array} \tag{16}$$

where a, b, c are localization maps. Recall that the 2-Selmer group

$$\mathrm{Sel}(J/k, 2) := \ker(c \circ \iota_*).$$

Proposition 5.4.1. *The 2-Selmer group $\mathrm{Sel}(J/k, 2) \subset \mathrm{H}^1(k, J[2])$ lies in $\ker\gamma$.*

Proof. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(k, J[2]) & \xrightarrow{\gamma} & \mathrm{H}^1(k, \mathrm{SO}(W)) \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle d} \\ \prod_v \mathrm{H}^1(k_v, J[2]) & \xrightarrow{(\gamma_v)} & \mathrm{H}^1(k_v, \mathrm{SO}(W)) \end{array}$$

where d is also the localization map. Suppose $\alpha \in \mathrm{Sel}(J/k, 2)$. Then $b(\alpha)$ is in the image of δ. Proposition 4.2.1 and the above diagram imply

$$d(\gamma(\alpha)) = 0.$$

But Hasse-Minkowski theorem says d is injective. Hence $\gamma(\alpha) = 0$ as desired.

□

In previous sections, we have seen that $\ker \gamma$ are finite in the cases where its order cam be estimated. However, in general $\ker \gamma$ is not always finite. We give a counterexample below.

Counterexample 5.4.2. Let $k = \mathbb{Q}$, and $f(x) = (x-1)(x^{2n} - 3)$.
For each $d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, consider the twisted hyper elliptic curve with affine equation

$$C_d : \ dy^2 = f(x).$$

and let J_d denote the Jacobian variety. Then as Galois modules

$$J_d[2](\mathbb{Q}^s) = J[2](\mathbb{Q}^s),$$

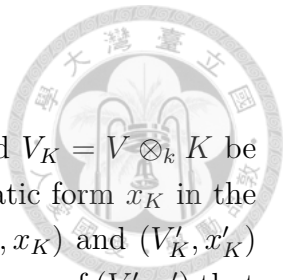
because both are generated by d_η as described in Lemma 4.1.2. Furthermore, by Proposition 5.4.1, the 2-Selmer group $\mathrm{Sel}(J_d/k, 2)$ of $\mathrm{H}^1(k, J_d[2]) = \mathrm{H}^1(k, J[2])$ also lies in $\ker \gamma$. The 2-Selmer groups of quadratic twists of such hyper-elliptic curve $y^2 = f(x)$ can be arbitrarily large [Chang, Theorem 5.5]. Hence $\ker \gamma$ does contain infinitely many elements.

6. Appendix

6.1. **Special case of Galois descent.**

Let V be a vector space over a field k with a fixed non-degenerate quadratic form x. Two pairs (V, x) and (V', x') are called k-isomorphic if there is a k-linear isomorphism

$$f : V \to V'$$



such that $f(x) = x'$.

Let K/k be a finite Galois extension with Galois group G,and $V_K = V \otimes_k K$ be the vector space over K. The quadratic form x defines a quadratic form x_K in the obvious way.We say (V, x) and (V', x') are K-isomorphic if (V_K, x_K) and (V'_K, x'_K) are isomorphic. Denote by $E_V(K/k)$ the set of k-isomorphism classes of (V', x') that are K-isomorphic to (V, x).

Let A_K be the group of K-automorphisms of (V_K, x_K). The group G acts on A_K as follows: $s \in G$ acts on V_K by $s(x \otimes \lambda) = x \otimes s(\lambda)$. Now if $f : V_K \to V_K$ is a linear map, put $s(f)(x) = s(f(s^{-1}(x)))$.

So let $(V', x') \in E_V(K, k)$ and $f : V_K \to V'_K$ be a K-isomorphism.For each $s \in G$,put

$$p_s = f^{-1} \circ s(f) = f^{-1} \circ s \circ f \circ s^{-1}.$$

We have $p_s \in A_K$. The map $s \mapsto p_s$ is a 1-cocycle,and changing f gives another p_s that differs from the original p_s by a 1-coboundary. Hence we have defined a map

$$\theta : E_V(K/k) \to H^1(G, A_K)$$

Also note that here A_K is actually the orthogonal group $O_K(x)$ of the quadratic form x over K.

Proposition 6.1.1. *The map θ is bijective.*

Proof. To show θ is injective. Let (V'_1, x'_1) and (V'_2, x'_2) correspond to the same cocycle p_s. And let f_1,f_2 be the corresponding K-isomorphisms. Then

$$f_1^{-1} \circ s(f_1) = f_2^{-1} \circ s(f_2).$$

Hence $s(f_2 f_1^{-1}) = f_2 f_1^{-1}$, and the map $f_2 f_1^{-1}$ is a k-isomorphism from (V'_1, x'_1) to (V'_2, x'_2).Thus θ is injective.

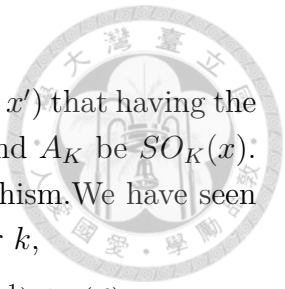
To show θ is surjective.Let p_s be a 1-cocycle of G with values in A_K. Because $A_K \subset GL(V_K)$ and $H^1(G, GL(V_K)) = 1$, there is a K-automorphism f of V_K such that

$$p_s = f^{-1} \circ s(f)$$

for all $s \in G$.And put $x' = f(x)$,x' is defined over k. Indeed, for all $s \in G$,we have

$$s(x') = s(f)(s(x)) = s(f)(x) = f \circ p_s(x) = f(x) = x'.$$

Hence $(V, x') \in E_V(K/k)$ and $\theta((V, x'))$ is equal to the class of p_s. □



Now we let $E'_V(K/k)$ be the set of k-isomorphism classes of (V', x') that having the same discriminant as (V, x) which are K-isomorphic to (V, x) and A_K be $SO_K(x)$. Then for $(V', x') \in E'_V(K/k)$ and $f : V_K \to V'_K$ be a K isomorphism.We have seen before that $p_s \in O_K(x)$. In this case, since $\det(f)$ is defined over k,

$$\det(p_s) = \det(f^{-1}) \det(s(f)) = \det(f^{-1})[s \cdot \det(f)] = \det(f^{-1}) \det(f) = 1.$$

Thus $p_s \in SO_K(x)$ and we can define $\theta : E'_V(K/k) \to H^1(G, SO_K(x))$ as before. Now the proof of bijectivity of θ is almost the same as the proof of Proposition 6.1.1. We only need to replace the statement "$A_K \subset GL_K(V)$" by "$A_K \subset SL_K(V)$" In the proof of surjectivity of θ.

Hence When $K = k^s$, U defined in Lemma 3.1.2, we have $H^1(k, SO(U))$=$\{k$-isomorphism classes of non-degenerate orthogonal spaces U' of dimension $2n$ with discriminant d over $k\}$.

And When $K = k^s$, W defined in Section 2, we have $H^1(k, SO(W))$= $\{k$-isomorphism classes of non-degenerate orthogonal spaces of dimension $2n + 1$ with determinant $(-1)^n$ over $k\}$.

References

[ABV] D.Mumford, *Abelian Varieties,* Oxford University Press, 1970

[AEC] J.H.Silverman, *The Arithmetic of Elliptic Curves,* Springer GTM 106, 1986

[SBF] J.Milnor and D.Husemoller, *Symmetric Bilinear Forms,* Springer Ergebnisse 73, 1970

[GC] J.P.Serre, *Galois Cohomology,* Springer Monographs in Mathematics, 1997

[Bhargava] M.Bhargava and B.H.Gross, *Arithmetic Invariant Theory,* Arxiv:1206.4774 , 2012

[TASM] M.Audin, *Torus Actions On Symplectic Manifolds*, Birkhäuser Progress in Mathematics, 2004

[Donagi] R.Donagi, *Group Law On The Intersection of Two Quadrics,* Annali della Scuola Normale Superiore di Pisa - Classe di Scienze 7.2 ,1980, 217-239

[Kottwiz] R.Kottwiz, *Stable trace formula: cuspidal tempered terms,* Duke Math. J. 51 ,1984, no. 3, 611–650.

[Chang] S.Chang, *On the arithmetic of twists of superelliptic curves,* Acta Arith 124 , 2006, 371–389

[GALA] S.H. Weintraub, *Guide To Advanced Linear Algebra,* Mathematical Association of America Guides #6, 2011

[ALA] S. Roman, *Advanced Linear Algebra,* Springer GTM 135, 2008

[AGS] W.C.Waterhouse, *Introduction to affine group schemes*, Springer GTM 66, 1979

[Wang] X.Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves,* Harvard Ph.D. thesis. 2013