Arithmetic invariant theory

Manjul Bhargava and Benedict H. Gross

August 7, 2012

Contents

1 Introduction

Let k be a field, let G be a reductive algebraic group over k, and let V be a linear representation of G. Geometric invariant theory involves the study of the k-algebra of G-invariant polynomials on V, and the relation between these invariants and the G-orbits on V, usually under the hypothesis that the base field k is algebraically closed. In favorable cases, one can determine the geometric quotient $V/\!\!/G = \mathrm{Spec}(\mathrm{Sym}^*(V^\vee))^G$ and can identify certain fibers of the morphism $V \to V/\!\!/G$ with certain G-orbits on V.

As an example, consider the three-dimensional adjoint representation of $G = \mathrm{SL}_2$ given by conjugation on the space V of 2×2 matrices $v = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ of trace zero. This is irreducible when

the characteristic of k is not equal to 2, which we assume here. It has the quadratic invariant $q(v) = -\det(v) = bc + a^2$, which generates the full ring of polynomial invariants. Hence $V/\!\!/G$ is isomorphic to the affine line and $q : V \to V/\!\!/G = \mathbb{G}_a$. If v and w are two vectors in V with $q(v) = q(w) \neq 0$, then they lie in the same G-orbit provided that the field k is separably closed.

For general fields the situation is more complicated. In our example, let d be a non-zero element of k and let K be the étale quadratic algebra $k[x]/(x^2 - d)$. Then the $G(k)$-orbits on the set of vectors $v \in V$ with $q(v) = d \neq 0$ can be identified with elements in the 2-group k^*/NK^*. (See §2.)

The additional complexity in the orbit picture, when k is not separably closed, is what we refer to as arithmetic invariant theory. It can be reformulated using non-abelian Galois cohomology, but that does not give a complete resolution of the problem. Indeed, when the stabilizer G_v of v is smooth, we will see that there is a bijection between the different orbits over k which lie in the orbit of v over the separable closure and the elements in the kernel of the map in Galois cohomology $\gamma : H^1(k, G_v) \to H^1(k, G)$. Since γ is only a map of pointed sets, the computation of this kernel can be non-trivial.

In this paper, we will illustrate some of the issues which remain by considering the *regular semi-simple* orbits—i.e., the closed orbits whose stabilizers have minimal dimension—in three representations of the split odd special orthogonal group $G = \mathrm{SO}_{2n+1} = \mathrm{SO}(W)$ over a field k whose characteristic is not equal to 2. Namely, we will study:

- the standard representation $V = W$;
- the adjoint representation $V = \mathfrak{so}(W) = \wedge^2(W)$; and
- the symmetric square representation $V = \mathrm{Sym}^2(W)$.

In the first case, the map γ is an injection and the arithmetic invariant theory is completely determined by the geometric invariant theory. In the second case, the stabilizer is a maximal torus and the arithmetic invariant theory is the Lie algebra version of stable conjugacy classes of regular semi-simple elements. The theory of stable conjugacy classes, introduced by Langlands [13]–[14] and developed further by Shelstad [23] and Kottwitz [10], forms one of the key tools in the study of endoscopy and the trace formula. Here there are the analogous problems, involving the Galois cohomology of tori, for the adjoint representations of general reductive groups. In the third case, there are *stable* orbits in the sense of Mumford's geometric invariant theory [17], i.e., closed orbits whose stabilizers are finite. Such representations arise more generally in Vinberg's invariant theory (cf. [20], [18]), where the torsion automorphism corresponds to a regular elliptic class in the extended Weyl group. In this case, we can use the geometry of pencils of quadrics to describe an interesting subgroup of classes in the kernel of γ.

Although we have focused here primarily on the case of orbits over a general field, a complete arithmetic invariant theory would also consider the orbits of a reductive group over more general rings such as the integers. We end with some remarks on integral orbits for the three representations we have discussed.

We would like to thank Brian Conrad, for his help with étale and flat cohomology, and Mark Reeder and Jiu-Kang Yu for introducing us to Vinberg's theory. We would also like to thank Bill Casselman, Wei Ho, Alison Miller, Jean-Pierre Serre, and the anonymous referee for a number of very useful comments on an earlier draft of this paper. It is a pleasure to dedicate this paper to Nolan Wallach, who introduced one of us (BHG) to the beauties of invariant theory.

2 Galois cohomology

Let k be a field, let k^s be a separable closure of k, and let k^a denote an algebraic closure containing k^s. Let Γ be the (profinite) Galois group of k^s over k. Let G be a reductive group over k and V an algebraic representation of G on a finite-dimensional k-vector space. The problem of classifying the $G(k)$-orbits on $V(k)$ which lie in a fixed $G(k^s)$-orbit can be translated (following Serre [21, §I.5]) into the language of Galois cohomology.

Let $v \in V(k)$ be a fixed vector in this orbit, and let G_v be the stabilizer of v. We assume that G_v is a smooth algebraic group over k. If $w \in V(k)$ is another vector in the same $G(k^s)$-orbit as v, then we may write $w = g(v)$ with $g \in G(k^s)$ well-defined up to right multiplication by $G_v(k^s)$. For every $\sigma \in \Gamma$, we have $g^\sigma = ga_\sigma$ with $a_\sigma \in G_v(k^s)$. The map $\sigma \to a_\sigma$ is a continuous 1-cocycle on Γ with values in $G_v(k^s)$, whose class in the first cohomology set $H^1(\Gamma, G_v(k^s))$ is independent of the choice of g. Since $a_\sigma = g^{-1}g^\sigma$, this class is trivial when mapped to the cohomology set $H^1(\Gamma, G(k^s))$. We will use the notation $H^1(k, G_v)$ and $H^1(k, G)$ to denote these Galois cohomology sets in this paper.

Reversing the argument, one can show similarly that an element in the kernel of the map of pointed sets $H^1(k, G_v) \to H^1(k, G)$ gives rise to a $G(k)$-orbit on $V(k)$ in the $G(k^s)$-orbit of v. Hence we obtain the following.

Proposition 1 *There is a bijection between the set of $G(k)$-orbits on the vectors w in $V(k)$ that lie in the same $G(k^s)$-orbit as v and the kernel of the map*

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

in Galois cohomology.

When the stabilizer G_v is smooth over k, the set of all vectors $w \in V(k)$ lying in the same $G(k^s)$-orbit as v can be identified with the k-points of the quotient variety G/G_v, and the central problem of arithmetic invariant theory in this case is to understand the kernel of the map γ in Galois cohomology. This is particularly interesting when k is a finite, local, or global field, when the cohomology of the two groups G_v and G can frequently be computed.

In the example of the introduction with $G = \mathrm{SL}_2$ and V the adjoint representation (again assuming $\mathrm{char}(k) \neq 2$), let v be a vector in $V(k)$ with $q(v) = d \neq 0$. Then the stabilizer G_v is a maximal torus in SL_2 which is split by the étale quadratic algebra K. The pointed set $H^1(k, G) = H^1(k, \mathrm{SL}_2)$ is trivial, so all classes in the abelian group $H^1(k, G_v) = k^*/NK^*$ lie in the kernel of γ. These classes index the orbits of $\mathrm{SL}_2(k)$ on the set S of non-zero vectors w with $q(w) = q(v)$, since this is precisely the set S of vectors $w \in V(k)$ which lie in the same $\mathrm{SL}_2(k^s)$-orbit as v. (This illustrates the point that one first has to solve the orbit problem over the separable closure k^s, before using Proposition 1 to descend to orbits over k.)

The vanishing of $H^1(k, G)$ occurs whenever $G = \mathrm{GL}_n$ or $G = \mathrm{SL}_n$ or $G = \mathrm{Sp}_{2n}$, and gives an elegant solution to many orbit problems. For example, when the characteristic of k is not equal to 2, the classification of the non-degenerate orbits of $\mathrm{SL}_n = \mathrm{SL}(W)$ on the symmetric square representation $V = \mathrm{Sym}^2(W^\vee)$ shows that the isomorphism classes of non-degenerate orthogonal spaces W of dimension n over k with a fixed determinant in k^*/k^{*2} correspond bijectively to classes in $H^1(k, G_v) = H^1(k, \mathrm{SO}(W))$ (cf. [11, Ch VII, §29], [21, Ch III, Appendix 2, §4]). In general, both $H^1(k, G_v)$ and $H^1(k, G)$ are non-trivial, and the determination of the kernel of γ remains a challenging problem.

Remark 2 In those cases where the stabilizer G_v is not smooth, it is at least flat of finite type over k, so one can replace the map γ in Galois (étale) cohomology with one in flat (fppf) cohomology. Indeed, the k-valued points of G/G_v can always be identified with the possibly larger set S' of vectors w' in $V(k)$ which lie in the same $G(k^a)$-orbit as v, where k^a is an algebraic closure of k^s. As an example, the group $\mathbb{G}_m$ acts on $V = \mathbb{G}_a$ by the formula $\lambda(v) = \lambda^p \cdot v$. The stabilizer of $v = 1$ is the subgroup μ_p, and $G/G_v = \mathbb{G}_m/\mu_p = \mathbb{G}_m$. The stabilizer G_v is smooth if the characteristic of k is not equal to p, in which case the set S consists of the non-zero elements of the field k, and the $G(k)$-orbits on S form a principal homogeneous space for the group $H^1(k, \mu_p) = k^*/k^{*p}$. If the characteristic of k is equal to p, the stabilizer μ_p is not smooth over k. In this case the set S consists of the p^{th} powers in k^*. The set S' is equal to the full group of non-zero elements in k, which is strictly larger than S when the field k is imperfect. In the general case one can show that the $G(k)$ orbits on $S' = (G/G_v)(k)$ are in bijection with the kernel of the map $\gamma_f : H^1_f(k, G_v) \to H^1_f(k, G)$ in flat (fppf) cohomology. In our example, we get a bijection of these orbits with the flat cohomology group $H^1_f(k, \mu_p) = k^*/k^{*p}$, as $H^1_f(k, \mathbb{G}_m) = 1$.

The semi-simple orbits in the three representations that we will study in this paper all have smooth stabilizers G_v. Hence we only consider the map γ in Galois cohomology.

3 Some representations of the split odd special orthogonal group

Let k be a field, with $\text{char}(k) \neq 2$. Let $n \geq 1$ and let W be a fixed non-degenerate, split orthogonal space over k, of dimension $2n + 1 \geq 3$ and determinant $(-1)^n$ in k^*/k^{*2}. Such an orthogonal space is unique up to isomorphism. If $\langle v, w\rangle$ is the bilinear form on W, then we may choose an ordered basis $\{e_1, e_2, \ldots, e_n, u, f_n, \ldots, f_2, f_1\}$ of W over k with inner products given by

$$\begin{aligned} \langle e_i, e_j\rangle = \langle f_i, f_j\rangle = \langle e_i, u\rangle = \langle f_i, u\rangle = 0, \\ \langle e_i, f_j\rangle = \delta_{ij}, \\ \langle u, u\rangle = 1. \end{aligned} \tag{2}$$

The Gram matrix of the bilinear form with respect to this basis (which we will call *the standard basis*) is an anti-diagonal matrix. (A good general reference on orthogonal spaces, which gives proofs of these results, is [16].)

Let $T : W \to W$ be a k-linear transformation. We define the *adjoint transformation* T^* by the formula

$$\langle Tv, w\rangle = \langle v, T^*w\rangle.$$

The matrix of T^* in our standard basis is obtained from the matrix of T by reflection around the anti-diagonal. In particular, we have the identity $\det(T) = \det(T^*)$. We say a linear transformation $g : W \to W$ is *orthogonal* if $\langle gv, gw\rangle = \langle v, w\rangle$. Then g is invertible, with $g^{-1} = g^*$, and $\det(g) = \pm 1$ in k^*. We define the *special orthogonal group* $\mathrm{SO}(W)$ of W by

$$\mathrm{SO}(W) := \{g \in \mathrm{GL}(W) : gg^* = g^*g = 1,\ \det(g) = 1\}. \tag{3}$$

We are going to consider the arithmetic invariant theory for three representations V of the reductive group $G = \mathrm{SO}(W)$ over k.

The first is the standard representation $V = W$, which is irreducible and symmetrically self-dual (isomorphic to its dual by a symmetric bilinear pairing) of dimension $2n + 1$. Here we will see that

the invariant polynomial $q_2(v) := \langle v, v\rangle$ generates the ring of polynomial invariants and separates the non-zero orbits over k.

The second is the adjoint representation $V = \mathfrak{so}(W)$, which is irreducible and symmetrically self-dual of dimension $2n^2 + n$. This representation is isomorphic to the exterior square $\wedge^2(W)$ of W, and can be realized as the space of skew self-adjoint operators:

$$V = \wedge^2(W) = \{T : W \to W : T = -T^*\}, \tag{4}$$

where $g \in G$ acts by conjugation: $T \mapsto gTg^{-1} = gTg^*$. The Lie bracket on V is given by the formula $[T_1, T_2] = T_1T_2 - T_2T_1$ and the duality by $\langle T_1, T_2\rangle = \mathrm{Trace}(T_1T_2)$. Here the theory of $G(k)$-orbits in a fixed $G(k^s)$-orbit is the Lie algebra version of stable conjugacy classes for the group $G = \mathrm{SO}(W)$.

The third is a representation V which arises in Vinberg's theory, from an outer involution θ of the group $\mathrm{GL}(W)$. It is isomorphic to the symmetric square $\mathrm{Sym}^2(W)$ of W, and can be realized as the space of self-adjoint operators:

$$V = \mathrm{Sym}^2(W) = \{T : W \to W : T = T^*\}, \tag{5}$$

where again $G = \mathrm{SO}(W)$ acts by conjugation. This representation has dimension $2n^2 + 3n + 1$ and is symmetrically self-dual by the pairing $\langle T_1, T_2\rangle = \mathrm{Trace}(T_1T_2)$. We will see that there are stable orbits, and that the arithmetic invariant theory of the stable orbits involves the arithmetic of hyperelliptic curves of genus n over k, with a k-rational Weierstrass point.

We note that the third representation V is not irreducible, as it contains the trivial subspace spanned by the identity matrix, and has a non-trivial invariant linear form given by the trace. When the characteristic of k does not divide $2n + 1 = \dim(W)$, the representation V is the direct sum of the trivial subspace and the kernel of the trace map, and the latter is irreducible and symmetrically self-dual of dimension $2n^2 + 3n$. When the characteristic of k divides $2n + 1$ the trivial subspace is contained in the kernel of the trace. In this case V has two trivial factors and an irreducible factor of dimension $2n^2 + 3n - 1$ in its composition series.

4 Invariant polynomials and the discriminant

In the standard representation $V = W$ of $G = \mathrm{SO}(W)$, the quadratic invariant $q_2(v) = \langle v, v\rangle$ generates the ring of invariant polynomials. We define $\Delta = q_2$ in this case. When $\Delta(v) \neq 0$, the stabilizer G_v is the reductive subgroup $\mathrm{SO}(U)$, where U is the hyperplane in W of vectors orthogonal to v.

In the second and third representations, the group $\mathrm{SO}(W)$ acts by conjugation on the subspace V of $\mathrm{End}(W)$. Hence the characteristic polynomial of an operator T is an invariant of the $G(k)$-orbit.

For the adjoint representation, the operator T is skew self-adjoint and its characteristic polynomial has the form

$$f(x) = \det(xI - T) = x^{2n+1} + c_2x^{2n-1} + c_4x^{2n-3} + \cdots + c_{2n}x = xg(x^2).$$

with coefficients $c_{2m} \in k$. The coefficients c_{2m} are polynomial invariants of the representation, with $\deg(c_{2m}) = 2m$. These polynomials are algebraically independent and generate the full ring of polynomial invariants on $V = \mathfrak{so}(W)$ over k [3, Ch 8, §8.3, §13.2, VI].. An important polynomial invariant, of degree $2n(2n + 1)$, is the discriminant Δ of the characteristic polynomial of T:

$$\Delta = \Delta(c_2, c_4, \ldots, c_{2n}) = \mathrm{disc}\, f(x).$$

This is non-zero in k precisely when the polynomial $f(x)$ is separable, so has $2n+1$ distinct roots in the separable closure k^s of k. The condition $\Delta(T) \neq 0$ defines the regular semi-simple orbits in the Lie algebra. For such an orbit, we will see that the stabilizer G_T is a maximal torus in G, of dimension n over k.

For the third representation V on self-adjoint operators, the characteristic polynomial $f(x)$ of T can be any monic polynomial of degree $2n+1$; we write

$$f(x) = \det(xI - T) = x^{2n+1} + c_1 x^{2n} + c_2 x^{2n-1} + \cdots + c_{2n} x + c_{2n+1}$$

with coefficients $c_m \in k$. Again the c_m give algebraically independent polynomial invariants, with $\deg(c_m) = m$, which generate the full ring of polynomial invariants on V over k. The discriminant

$$\Delta = \Delta(c_1, c_2, \ldots, c_{2n+1}) = \operatorname{disc} f(x)$$

is defined as before, and is non-zero when $f(x)$ is separable. We will see that the condition $\Delta(T) \neq 0$ defines the stable orbits of G on V. For such an orbit, we will see that the stabilizer G_T is a finite commutative group scheme of order 2^{2n} over k, which embeds as a Jordan subgroup scheme of G (see [12, Ch 3]).

5 The orbits with non-zero discriminant

In this section, for each of the three representations V, we exhibit an orbit for G where the invariant polynomials described above take arbitrary values in k, subject to the single restriction that $\Delta \neq 0$. We calculate the stabilizer G_v and its cohomology $H^1(k, G_v)$ in terms of the values of the invariant polynomials on v. We also give an explicit description of the map $\gamma : H^1(k, G_v) \to H^1(k, G)$. We note that all three representations arise naturally in Vinberg's invariant theory, and the representative orbits that we will construct are in the Kostant section (cf. [18]).

When $V = W$ is the standard representation, let d be an element of k^*. The vector $v = e_1 + df_1$ has $q_2(v) = \Delta(v) = d$. The stabilizer G_v acts on the orthogonal complement U of the non-degenerate line kv in W, which is a quasi-split orthogonal space of dimension $2n$ and discriminant d in k^*/k^{*2}. (The *discriminant* of an orthogonal space of dimension $2n$ is defined as $(-1)^n$ times its determinant.) This gives an identification $G_v = \mathrm{SO}(U)$, where the special orthogonal group $\mathrm{SO}(U)$ is quasi-split over k and split by $k(\sqrt{d})$. Witt's extension theorem [16, Ch 1] shows that all vectors w with $q_2(w) = d$ lie in the $G(k)$-orbit of v, so the invariant polynomials separate the orbits over k with non-zero discriminant. One can also show that there is a single non-zero orbit with $q_2(v) = 0$, represented by the vector $v = e_1 = e_1 + 0f_1$.

The cohomology set $H^1(k, \mathrm{SO}(U))$ classifies non-degenerate orthogonal spaces U' of dimension $2n$ and discriminant d over k, and the cohomology set $H^1(k, \mathrm{SO}(W))$ classifies non-degenerate orthogonal spaces W' of dimension $2n+1$ and determinant $(-1)^n$ over k, with the trivial class corresponding to the split space W. The map

$$\gamma : H^1(k, G_v) = H^1(k, \mathrm{SO}(U)) \longrightarrow H^1(k, G) = H^1(k, \mathrm{SO}(W))$$

is given explicitly by mapping the space U' to the space $W' = U' + \langle d \rangle$. Witt's cancellation theorem [16] shows that the map γ is an injection of sets in this case, so the arithmetic invariant theory for the standard representation of any odd orthogonal group is the same as its geometric invariant theory.

For the second representation $V = \mathfrak{so}(W) = \wedge^2(W)$, let

$$f(x) = x^{2n+1} + c_2 x^{2n-1} + c_4 x^{2n-3} + \cdots + c_{2n} x$$

be a polynomial in $k[x]$ with non-zero discriminant. We will construct a skew self-adjoint operator T on W with characteristic polynomial $f(x)$. Since $f(x) = xh(x) = xg(x^2)$, we have

$$\operatorname{disc} f(x) = c_{2n}^2 \operatorname{disc} h(x) = (-4)^n c_{2n}^3 \operatorname{disc} g(x)^2.$$

Let $K = k[x]/(g(x))$, $E = k[x]/(h(x))$, and $L = k[x]/(f(x))$. By our assumption that $\Delta \neq 0$, these are étale k-algebras of ranks n, $2n$, and $2n+1$ respectively. We have $L = E \oplus k$. Furthermore the map $x \to -x$ induces an involution τ of the algebras E and of L, with fixed algebras K and $K \oplus k$ respectively.

Let β be the image of x in $L = k[x]/(f(x))$, so $f(\beta) = 0$ in L and $f'(\beta)$ is a unit in L^*, We define a symmetric bilinear form $\langle\ ,\ \rangle$ on the k-vector space $L = k + k\beta + k\beta^2 + \cdots + k\beta^{2n}$ by taking

$$\langle \lambda, \mu \rangle := \text{ the coefficient of } \beta^{2n} \text{ in the product } (-1)^n \lambda \mu^\tau. \tag{6}$$

This is non-degenerate, of determinant $(-1)^n$, and the map $t(\lambda) = \beta\lambda$ is skew self-adjoint, with characteristic polynomial $f(x)$. Finally, the subspace $M = k + k\beta + \cdots + k\beta^{n-1}$ is isotropic of dimension n, so the orthogonal space L is split and isomorphic to W over k. Choosing an isometry $\theta : L \to W$ we obtain a skew self-adjoint operator $T = \theta t \theta^{-1}$ on W with the desired separable characteristic polynomial. Since the isometry θ is unique up to composition with an orthogonal transformation of W, the orbit of T is well-defined. The stabilizer of T in $\mathrm{O}(W)$ has k-points $\{\lambda \in L^* : \lambda^{1+\tau} = 1\}$. The subgroup G_T which fixes T is a maximal torus in $G = \mathrm{SO}(W)$, isomorphic to the torus $\operatorname{Res}_{K/k} U_1(E/K)$ of dimension n over k.

Over the separable closure k^s of k, any skew self-adjoint operator S with (separable) characteristic polynomial $f(x)$ is in the same orbit of T. Indeed, since $f(x)$ is separable, it is also the minimal polynomial of T and S, so we can find an element g in $\mathrm{GL}(W)$ with $S = gTg^{-1}$. Since both operators are skew self-adjoint, the product g^*g is in the centralizer of T in $\mathrm{GL}(W)$. The centralizer of T in $\mathrm{End}(W)$ is the algebra $k[T] = L$. Since g^*g is self-adjoint in L^*, and its determinant is a square in k^*, we see that g^*g is an element of the subgroup $K^* \times k^{*2}$. Over the separable closure, every element of $K^* \times k^{*2}$ is a norm from L^*: $g^*g = h^{1+\tau}$. Then gh^{-1} is an orthogonal transformation of W over k^s mapping T to S. Hence S is in the $\mathrm{SO}(W)(k^s)$-orbit of T.

To understand the orbits with a fixed separable characteristic polynomial over k, we need an explicit form of the map γ in Galois cohomology. Since the stabilizer of T is abelian, the pointed set $H^1(k, G_T)$ is an abelian group, which is isomorphic to K^*/NE^* by Hilbert's Theorem 90. The map

$$\gamma : K^*/NE^* = H^1(k, G_T) \longrightarrow H^1(k, G) = H^1(k, \mathrm{SO}(W))$$

is given explicitly as follows. We first associate to an element $\kappa \in K^*$ the element $\alpha = (\kappa, 1)$ in $(L^\tau)^* = K^* \times k^*$, with square norm from L^* to k^*. We then associate to α the vector space L with symmetric bilinear form

$$\langle \lambda, \mu \rangle_\alpha := \text{the coefficient of } \beta^{2n} \text{ in the product } (-1)^n \alpha \lambda \mu^\tau. \tag{7}$$

This orthogonal space W_κ has dimension $2n+1$ and determinant $(-1)^n$ over k, and its isomorphism class depends only on the class of κ in the quotient group $K^*/NE^* = H^1(k, G_T)$.

Lemma 3 *The orthogonal space W_κ represents the class $\gamma(\kappa)$ in $H^1(k, \mathrm{SO}(W))$.*

Proof: We first recall the recipe for associating to a cocycle g_σ on the Galois group with values in $\mathrm{SO}(W)(k^s)$ a new orthogonal space W' over k. We use the inclusion $\mathrm{SO}(W) \to \mathrm{GL}(W)$ and the triviality of $H^1(k, \mathrm{GL}(W))$ to write $g_\sigma = h^{-1}h^\sigma$ for an element $h \in \mathrm{GL}(W)(k^s)$. We then define a new non-degenerate symmetric bilinear form on W by the formula

$$\langle v, w\rangle^* = \langle h^{-1}v, h^{-1}w\rangle. \tag{8}$$

This takes values in k and defines the space W', which has dimension $2n+1$ and determinant $(-1)^n$. The isomorphism class of W' over k depends only on the cohomology class of the cocycle g_σ in $H^1(k, \mathrm{SO}(W))$.

In our case, the cocycle g_σ representing $\gamma(\kappa)$ comes from a cocycle with values in the stabilizer G_v. This is a maximal torus in $\mathrm{SO}(W)$, which is a subgroup of the maximal torus $\mathrm{Res}_{L/k}\mathbb{G}_m$ of $\mathrm{GL}(W)$. This torus already has trivial Galois cohomology, so we can write $g_\sigma = h^\sigma/h$ with $h \in (L \otimes k^s)^*$ satisfying $h^{1+\tau} = \alpha$. Substituting this particular h into formula (8) for the new inner product on W completes the proof. □

We note that the class κ above will be in the kernel of γ precisely when the quadratic space W' with bilinear form $\langle\ ,\ \rangle_\alpha$ is split. Such classes give additional orbits of $\mathrm{SO}(W)$ on $\mathfrak{so}(W) = \wedge^2(W)$ over k with characteristic polynomial $f(x)$.

The analysis for the third representation $V = \mathrm{Sym}^2(W)$ is similar. Here we start with an arbitrary monic separable polynomial $f(x) = x^{2n+1} + c_1x^{2n} + \cdots + c_{2n+1}$ and wish to construct a self-adjoint operator T on W with characteristic polynomial $f(x)$. We let $L = k[x]/(f(x))$, which is an étale k-algebra of rank $2n+1$, and let β be the image of x in L. We define a symmetric bilinear form $\langle\lambda, \mu\rangle$ on $L = k + k\beta + \cdots + k\beta^{2n}$ by taking the coefficient of β^{2n} in the product $\lambda\mu$. This is non-degenerate of determinant $(-1)^n$, and the map $t(\lambda) = \beta\lambda$ is self-adjoint, with characteristic polynomial $f(x)$. Finally, the subspace $M = k + k\beta + \cdots + k\beta^{n-1}$ is isotropic of dimension n, so the orthogonal space L is split and isomorphic to W over k. Choosing an isometry $\theta : L \to W$, we obtain a self-adjoint operator $T = \theta t\theta^{-1}$ on W with the desired separable characteristic polynomial. Since the isometry θ is unique up to composition with an orthogonal transformation of W, the orbit of T is well-defined. The stabilizer of T in $\mathrm{O}(W)$ has k-points $\{\lambda \in L^* : \lambda^2 = 1\}$. The subgroup G_T in $\mathrm{SO}(W)$ which fixes T is the finite étale group scheme A of order 2^{2n}, which is the kernel of the norm map $\mathrm{Res}_{L/k}(\mu_2) \to \mu_2$.

Over the separable closure k^s of k, any self-adjoint operator S with (separable) characteristic polynomial $f(x)$ is in the same orbit as T. Indeed, since $f(x)$ is separable, it is also the minimal polynomial of T and S, so we can find an element $g \in \mathrm{GL}(W)$ with $S = gTg^{-1}$. Since both operators are self-adjoint, the product g^*g is in the centralizer of T in $\mathrm{GL}(W)$. The centralizer of T in $\mathrm{End}(W)$ is the algebra $k[T] = L$, so g^*g is an element of L^*. Over the separable closure, every element of L^* is a square: $g^*g = h^2$. Then gh^{-1} is an orthogonal transformation of W over k^s mapping T to S. Hence S is in the $\mathrm{SO}(W)(k^s)$-orbit of T.

We now consider the orbits with a fixed separable characteristic polynomial over k. Since the stabilizer of T is again abelian, the pointed set $H^1(k, G_T)$ is an abelian group which is isomorphic to $(L^*/L^{*2})_{N=1}$ by Kummer theory. The map

$$\gamma : H^1(k, G_T) = (L^*/L^{*2})_{N=1} \longrightarrow H^1(k, G) = H^1(k, \mathrm{SO}(W))$$

is given explicitly as follows. We associate to an element α in $(L^*)_{N=1}$ the orthogonal space L with bilinear form $\langle \lambda, \mu \rangle_\alpha$ given by the coefficient of β^{2n} in the product $\alpha\lambda\mu$. This orthogonal space has dimension $2n+1$ and determinant $(-1)^n$ over k. Its isomorphism class over k depends only on the image of α in the quotient group $(L^*/L^{*2})_{N=1} = H^1(k, G_T)$. This orthogonal space represents the class $\gamma(\alpha)$ in $H^1(k, \mathrm{SO}(W))$. The proof is the same as that of Lemma 3. We first observe that the map taking the cocycle g_σ from G_T to $\mathrm{SO}(W)$ to $\mathrm{GL}(W)$ can also be obtained by mapping G_T to the maximal torus $\mathrm{Res}_{L/k}\, \mathbb{G}_m$ in $\mathrm{GL}(W)$. This torus has trivial cohomology, so $\alpha = h^2$ with $h \in (L \otimes k^s)^*$, and this choice of h gives the inner product $\langle \lambda, \mu \rangle_\alpha$. The class α will be in the kernel of γ precisely when the quadratic space L with bilinear form $\langle\ ,\ \rangle_\alpha$ is split; such classes give additional orbits of $\mathrm{SO}(W)$ on $\mathrm{Sym}^2(W)$ over k with characteristic polynomial $f(x)$.

We summarize what we have established for the representations $V = \mathfrak{so}(W)$ and $V = \mathrm{Sym}^2(W)$.

Proposition 4 *For each monic separable polynomial $f(x)$ of degree $2n+1$ over k of the form $f(x) = xg(x^2)$ there is a distinguished $\mathrm{SO}(W)(k)$-orbit of skew self-adjoint operators T on W with characteristic polynomial $f(x)$. All other orbits on $\wedge^2(W)$ with this characteristic polynomial lie in the $\mathrm{SO}(W)(k^s)$-orbit of T, and correspond bijectively to the non-identity classes in the kernel of $\gamma : K^*/NE^* \to H^1(k, \mathrm{SO}(W))$, where $K = k[x]/(g(x))$ and $E = k[x]/(g(x^2))$.*

For each monic separable polynomial $f(x)$ of degree $2n+1$ over k there is a distinguished $\mathrm{SO}(W)(k)$-orbit of self-adjoint operators T on W with characteristic polynomial $f(x)$. All other orbits on $\mathrm{Sym}^2(W)$ with this characteristic polynomial lie in the $\mathrm{SO}(W)(k^s)$-orbit of T, and correspond bijectively to the non-identity classes in the kernel of $\gamma : (L^*/L^{*2})_{N=1} \to H^1(k, \mathrm{SO}(W))$, where $L = k[x]/(f(x))$.

6 Stable orbits and hyperelliptic curves

For both representations $V = \wedge^2(W)$ and $V = \mathrm{Sym}^2(W)$ of $G = \mathrm{SO}(W)$ we associated to the distinguished orbit T with separable characteristic polynomial $f(x)$ and any class α in the cohomology group $H^1(k, G_T)$ a symmetric bilinear form $\langle \lambda, \mu \rangle_\alpha$ on the k-vector space $L = k[x]/(f(x))$. The class α is in the kernel of the map $\gamma : H^1(k, G_T) \to H^1(k, G)$ precisely when this quadratic space is split over k. However, exhibiting specific classes $\alpha \neq 1$ where this space is split is a difficult general problem, so it is difficult to exhibit other orbits with this characteristic polynomial.

In the case of the third representation $V = \mathrm{Sym}^2(W)$, the orbits T with $\Delta(T) \neq 0$ are stable; namely, they are closed (defined by the values of the invariant polynomials over the separable closure) and have finite stabilizer (the commutative group scheme $A = \mathrm{Res}_{L/k}(\mu_2)_{N=1}$ of order 2^{2n}). In this case, we will use some results in algebraic geometry, on hyperelliptic curves with a Weierstrass point and the Fano variety of the complete intersection of two quadrics in $\mathbb{P}(L \oplus k)$, to produce certain classes in the kernel of the map $\gamma : H^1(k, A) \to H^1(k, \mathrm{SO}(W))$.

Let C be the smooth projective hyperelliptic curve of genus n over k with affine equation $y^2 = f(x)$ and k-rational Weierstrass point P above $x = \infty$. The functions on C which are regular outside of P form an integral domain:

$$H^0(C - P, O_{C-P}) = k[x, y]/(y^2 = f(x)) = k[x, \sqrt{f(x)}].$$

The complete curve C is covered by this affine open subset U_1, together with the affine open subset U_2 associated to the equation $w^2 = v^{2n+2} f(1/v)$ and containing the point $P = (0, 0)$. The

gluing of U_1 and U_2 is by $(v,w) = (1/x, y/x^{n+1})$ and $(x,y) = (1/v, w/v^{n+1})$ wherever these maps are defined. Let J denote the Jacobian of C over k and let $J[2]$ the kernel of multiplication by 2 on J. This is a finite étale group scheme of order 2^{2n} over k.

Lemma 5 *The group scheme $J[2]$ of 2-torsion on the Jacobian of C is canonically isomorphic to the stabilizer $A = \mathrm{Res}_{L/k}(\mu_2)_{N=1}$ of the orbit T in $\mathrm{SO}(W)$.*

Proof: Write $L = k[x]/(f(x)) = k + k\beta + \cdots + k\beta^{2n}$, where $f(\beta) = 0$. The other Weierstrass points $P_\eta = (\eta(\beta), 0)$ of $C(k^s)$ correspond bijectively to algebra embeddings $\eta : L \to k^s$. Associated to such a point we have the divisor $d_\eta = (P_\eta) - (P)$ of degree zero. The divisor class of d_η lies in the 2-torsion subgroup $J[2](k^s)$ of the Jacobian, as

$$2d_\eta = \mathrm{div}(x - \eta(\beta)).$$

The Riemann-Roch theorem shows that the classes d_η generate the finite group $J[2](k^s)$, and satisfy the single relation

$$\sum (d_\eta) = \mathrm{div}(y).$$

Since the Galois group of k^s acts on these classes by permutation of the embeddings η, we have an isomorphism of group schemes: $J[2] \cong \mathrm{Res}_{L/k}(\mu_2)/\mu_2$. This quotient of $\mathrm{Res}_{L/k}(\mu_2)$ is isomorphic to the subgroup scheme $A = \mathrm{Res}_{L/k}(\mu_2)_{N=1}$, as the degree of L over k is odd. This completes the proof. □

The exact sequence of Galois modules,

$$0 \to J[2](k^s) \to J(k^s) \to J(k^s) \to 0,$$

gives an exact descent sequence

$$0 \to J(k)/2J(k) \to H^1(k, J[2]) \to H^1(k, J)[2] \to 0$$

in Galois cohomology. By Lemma 5, the middle term in this sequence can be identified with the group $H^1(k, A) = H^1(k, G_T)$, and our main result in this section is the following.

Proposition 6 *The subgroup $J(k)/2J(k)$ of $H^1(k, A) = H^1(k, G_T)$ lies in the kernel of the map $\gamma : H^1(k, G_T) \to H^1(k, G)$.*

Proof: We first make the descent map from $H^1(k, A)$ to $H^1(k, J)[2]$ more explicit. That is, we need to associate to a class α in the group

$$H^1(k, A) = (L^*/L^{*2})_{N=1}$$

a principal homogeneous space F_α of order 2 for the Jacobian J over k. The class α will be in the subgroup $J(k)/2J(k)$ precisely when the homogeneous space F_α has a k-rational point.

We have previously associated to the class α the orthogonal space L with symmetric bilinear form $\langle \lambda, \mu \rangle_\alpha :=$ the coefficient of β^{2n} in the product $\alpha\lambda\mu$. We also defined a self-adjoint operator given by multiplication by β on L, and that gives a second symmetric bilinear form on L: $\langle \beta\lambda, \mu \rangle_\alpha = \langle \lambda, \beta\mu \rangle_\alpha$.

Let $M = L \oplus k$, which has dimension $2n+2$ over k, and consider the two quadrics on M given by

$$\begin{aligned} Q(\lambda, a) &= \langle \lambda, \lambda \rangle_\alpha \\ Q'(\lambda, a) &= \langle \beta\lambda, \lambda \rangle_\alpha + a^2. \end{aligned}$$

The pencil $uQ - vQ'$ is non-degenerate and contains exactly $2n+2$ singular elements over k^s, namely, the quadric Q at $v = 0$ and the $2n+1$ quadrics $\eta(\beta)Q - Q'$ at the points where $f(\eta(\beta)) = 0$. Hence the base locus is non-singular in $\mathbb{P}(M)$ and the Fano variety F_α of this complete intersection, consisting of the n-dimensional subspaces Z of M which are isotropic for all of the quadrics in the pencil, is a principal homogeneous space of order 2 for the Jacobian J (c.f. [7]). More precisely, there is a commutative algebraic group I_α with 2 components over k, having identity component J and non-identity component F_α.

Since the discriminant of the quadric $uQ - vQ'$ in the pencil is equal to $v^{2n+2}f(x)$ with $x = u/v$, a point $c = (x, y)$ on the hyperelliptic curve $y^2 = f(x)$ determines both a quadric $Q_x = xQ - Q'$ in the pencil together with a *ruling* of Q_x, i.e., a component of the variety of $(n+1)$-dimensional Q_x-isotropic subspaces in M. Each point gives an involution of the corresponding Fano variety $\theta(c) : F_\alpha \to F_\alpha$ with 2^{2n} fixed points over a separable closure k^s of k. The involution $\theta(c)$ is defined as follows. A point of F_α consist of a common isotropic subspace Z of dimension n in $M \otimes k^s$. The point c gives a maximal isotropic subspace Y for the quadric Q_x which contains Z. If we restrict any non-singular quadric in the pencil (other than Q_x) to Y, we get a reducible quadric which is the sum of two hyperplanes: Z and another common isotropic subspace Z'. This defines the involution: $\theta(c)(Z) = Z'$. In the algebraic group I_α, we have that $Z + Z'$ is the class of the divisor $(c) - (P)$ of degree zero in J.

Now assume that the class α is in the subgroup $J(k)/2J(k)$. Then its image in $H^1(k, J)$ is trivial, and the homogenous space F_α has a k-rational point. Hence there is a k-subspace Z of $M = L \oplus k$ which is isotropic for both Q and Q'. Since it is isotropic for Q', the subspace Z does not contain the line $0 \oplus k$, so its projection to the subspace L has dimension n and is isotropic for Q. This implies that the orthogonal space L with bilinear form $(\lambda, \nu)_\alpha$ is split, so the class α is in the kernel of the map $\gamma : H^1(k, A) \to H^1(k, \mathrm{SO}(W))$. $\square$

Note that when $c = P$, the Weierstrass point over $x = \infty$, the involution $\theta(P)$ is induced by the linear involution $(\lambda, a) \to (\lambda, -a)$ of $M = L \oplus k$. The fixed points are just the n-dimensional subspaces X over k^s which are isotropic for both quadrics

$$\begin{aligned} q(\lambda) &= \langle \lambda, \lambda \rangle_\alpha \,, \\ q'(\lambda) &= \langle \beta\lambda, \lambda \rangle_\alpha \end{aligned}$$

on the space L of dimension $2n+1$ over k. There are 2^{2n} such isotropic subspaces over k^s, and they form a principal homogeneous space for $J[2]$. The variety F_α has a k-rational point when α lies in the subgroup $J(k)/2J(k)$, but only has a k-rational point fixed by the involution $\theta(P)$ when α is the trivial class in $H^1(k, J[2])$.

Remark 7 The finite group scheme $A = J[2]$ does not determine the hyperelliptic curve C over k. Indeed, for any class $d \in k^*/k^{*2}$, the hyperelliptic curve C_d with affine equation $dy^2 = f(x)$ has the same 2-torsion subgroup of its Jacobian. This Jacobian J_d of C_d acts on the Fano variety of the

complete intersection of the two quadrics given by

$$\begin{aligned} Q(\lambda, a) &= \langle \lambda, \lambda \rangle_\alpha \,, \\ Q'(\lambda, a) &= \langle \beta\lambda, \lambda \rangle_\alpha + da^2. \end{aligned}$$

Indeed, the discriminant of the quadric $uQ - vQ'$ in the pencil is equal to $dv^{2n+2} f(x)$, where $x = u/v$. A similar argument then shows that the subgroup $J_d(k)/2J_d(k)$ is also contained in the kernel of the map γ on $H^1(k, A)$.

7 Arithmetic fields

In this section, we describe the orbits in our three representations when k is a finite, local, or global field.

7.1 Finite fields

First, we consider the case when k is finite, of odd order q. In this case, $H^1(k, \mathrm{SO}(W)) = 1$ by Lang's theorem, as $\mathrm{SO}(W)$ is connected. As a consequence, every quadratic space of dimension $2n+1$ and determinant $(-1)^n$ is split, and all elements of $H^1(k, G_T)$ lie in the kernel of γ.

In the standard representation $V = W$ the stabilizer of a vector v with $q_2(v) \neq 0$ is the connected orthogonal subgroup $\mathrm{SO}(U)$, which also has trivial first cohomology. So for every non-zero element d in k^*, there is a unique orbit of vectors with $q_2(v) = d$. (We have already seen this for general fields via Witt's extension theorem.)

In the adjoint representation $V = \mathfrak{so}(W)$, the stabilizer of a vector T with $\Delta(T) \neq 0$ is the connected torus $\mathrm{Res}_{K/k} U_1(E/K)$, which also has trivial first cohomology. So for each separable characteristic polynomial of the form $f(x) = xg(x^2)$ there is a unique orbit of skew self-adjoint operators T with characteristic polynomial $f(x)$.

In the representation $V = \mathrm{Sym}^2(W)$ the stabilizer of T with characteristic polynomial $f(x)$ satisfying $\mathrm{disc}(f) = \Delta(T) \neq 0$ is the finite group scheme $A = (\mathrm{Res}_{L/k} \mu_2)_{N=1}$. In this case $H^1(k, A) = (L^*/L^{*2})_{N=1}$ is an elementary abelian 2-group of order 2^m, where $m+1$ is the number of irreducible factors of $f(x)$ in $k[x]$. So 2^m is the number of distinct orbits with characteristic polynomial $f(x)$. But this is also the order of the stabilizer $H^0(k, A) = A(k) = (L^*[2])_{N=1}$ of any point in the orbit. Hence the number of self-adjoint operators T with any fixed separable polynomial is equal to the order of the finite group $\mathrm{SO}(W)(q)$. This is given by the formula

$$\#\,\mathrm{SO}(W)(q) = q^{n^2}(q^{2n} - 1)(q^{2n-2} - 1) \cdots (q^2 - 1).$$

By Lang's theorem, we also have $H^1(k, J) = 0$, where J is the Jacobian of the smooth hyperelliptic curve $y^2 = f(x)$ of genus n over k. Hence the homomorphism $J(k)/2J(k) \to H^1(k, A)$ is an isomorphism and every orbit with characteristic polynomial $f(x)$ comes from a k-rational point on the Jacobian.

7.2 Non-archimedean local fields

Next, we consider the case when k is a non-archimedean local field, with ring of integers O and finite residue field $O/\pi O$ of odd order. In this case, Kneser's theorem on the vanishing of H^1 for simply-

connected groups (cf. [19, Th. 6.4], [21]) gives an isomorphism

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

For the standard representation $V = W$, we also have $H^1(k, G_v) = H^1(k, \mathrm{SO}(U)) \cong (\mathbb{Z}/2\mathbb{Z})$, except in the case when $\dim(V) = 3$ and $q_2(v) = 1$, when $\mathrm{SO}(U)$ is a split torus and $H^1(k, \mathrm{SO}(U)) = 1$. The map γ is a bijection except in the special case.

For the adjoint representation $V = \mathfrak{so}(W)$, Kottwitz has shown in the local case that the map

$$\gamma : H^1(k, G_v) = (K^*/NE^*) \to H^1(k, G) = (\mathbb{Z}/2\mathbb{Z})$$

is actually a homomorphism of groups [10]. Let $f(x) = xg(x^2)$, so $K = k[x]/(g(x))$ and $E = k[x]/(g(x^2))$. It follows from local class field theory that the group K^*/NE^* is elementary abelian of order 2^m, where m is the number of irreducible factors $g_i(x)$ of $g(x)$ such that $g_i(x^2)$ remains irreducible over k. Kottwitz also shows that that the map γ is surjective when $m \geq 1$. Hence the number of orbits with separable characteristic polynomial $f(x)$ is 1 when $m = 0$, and is 2^{m-1} when $m \geq 1$.

For the third representation $V = \mathrm{Sym}^2(W)$, the map

$$\gamma : H^1(k, A) = H^1(k, J[2]) \to H^2(k, \mu_2) \cong (\mathbb{Z}/2\mathbb{Z})$$

is an even quadratic form. The associated bilinear form is the cup product on $H^1(k, J[2])$ induced from the Weil pairing $J[2] \times J[2] \to \mu_2$, and $J(k)/2J(k)$ is a maximal isotropic subspace on which $\gamma = 0$. This allows us to count the number of stable orbits with a fixed characteristic polynomial.

Let $m + 1$ be the number of irreducible factors of $f(x)$ in $k[x]$, and let O_L be the integral closure of the ring O in L. Then $H^1(k, A) = (L^*/L^{*2})_{N=1}$ has order 2^{2m} and the number of stable orbits with characteristic polynomial $f(x)$ is equal $2^{m-1}(2^m + 1) = 2^{2m-1} + 2^{m-1}$. The subgroup $J(k)/2J(k)$ has order 2^m, which is also the order of the subgroup $(O_L^*/O_L^{*2})_{N=1}$ of units. These two subgroups coincide when the polynomial $f(x)$ has coefficients in O and the quotient algebra $O[x]/(f(x))$ is maximal in L.

7.3 The local field $\mathbb{R}$

We next consider the orbits in our representations when $k = \mathbb{R}$ is the local field of real numbers. Then the pointed set $H^1(k, G) = H^1(k, \mathrm{SO}(W))$ has $n + 1$ elements, corresponding to the quadratic spaces W' of signature (p, q) satisfying: $p + q = 2n + 1$ and $q \equiv n \pmod 2$. The pointed set $H^1(k, G_v) = H^1(k, \mathrm{SO}(U))$ for the standard representation has $n + 1$ elements when $q_2(v)$ has sign $(-1)^n$, and has n elements when $q_2(v)$ has sign $-(-1)^n$. The map γ is a bijection in the first case and an injection in the second case, when the definite quadratic space W' does not have an orbit with $q_2(w^*) = q_2(v)$.

In the second and third representations, $H^1(k, G_T)$ is an elementary abelian 2-group, and we will consider the situations where it has maximal rank. For the adjoint representation $V = \mathfrak{so}(W)$, this occurs when all of the nonzero roots of the characteristic polynomial $f(x)$ of the skew self-adjoint transformation T are purely imaginary. Thus $f(x) = xg(x^2)$ where $g(x)$ factors completely over the real numbers and all of its roots are strictly negative. In this case, the 2-group $H^1(k, G_T) = K^*/NE^* = (\mathbb{R}^*)^n/N(\mathbb{C}^*)^n$ has rank n. The real orthogonal space W decomposes into n orthogonal T-stable planes and an orthogonal line on which $T = 0$. The signatures of these planes determine the real orbit of T. Writing $n = 2m$ or $n = 2m + 1$, we see that there are $\binom{n}{m}$ elements in the kernel of

γ. One can show that γ is surjective in this case, and calculate the order of each fiber as a binomial coefficient $\binom{n}{k}$.

For the symmetric square representation $V = \mathrm{Sym}^2(W)$, the 2-group $H^1(k, G_T)$ has maximal rank when the characteristic polynomial $f(x)$ of the self-adjoint transformation T factors completely over the real numbers. In this case, $H^1(k, G_T) = ((\mathbb{R}^*)^{2n+1}/(\mathbb{R}^{*2})^{2n+1})_{N=1}$ has rank $2n$. The real orthogonal space W decomposes into $2n+1$ orthogonal eigenspaces for T, and the signatures of these lines determine the real orbit. Hence there are $\binom{2n+1}{n}$ elements in the kernel of γ. One can also show that γ is surjective in this case, and calculate the order of each fiber as a binomial coefficient $\binom{2n+1}{k}$ with $k \equiv n \pmod 2$.

7.4 Global fields

Finally, we consider the representation $\mathrm{Sym}^2(V)$ when k is a global field. In this case, the group $H^1(k, A) = H^1(k, J[2])$ is infinite. We will now prove that there are also infinitely many classes in the kernel of γ, so infinitely many orbits with characteristic polynomial $f(x)$.

Proposition 8 *Every class α in the 2-Selmer group $\mathrm{Sel}(J/k, 2)$ of $H^1(k, J[2])$ lies in the kernel of γ, so corresponds to an orbit over k.*

Proof: By definition, the elements of the 2-Selmer group $\mathrm{Sel}(J/k, 2)$ correspond to classes in $H^1(k, J[2])$ whose restriction to $H^1(k_v, J[2])$ is in the image of $J(k_v)/2J(k_v)$ for every completion k_v. Hence the orthogonal space U_v associated to the class $\gamma(\alpha_v)$ in $H^1(k_v, \mathrm{SO}(V))$ is split at every completion k_v. By the theorem of Hasse and Minkowski, a non-degenerate orthogonal space U of dimension $2n+1$ is split over k if and only if $U_v = U \otimes k_v$ is split over every completion k_v. Hence the orthogonal space U associated to $\gamma(\alpha)$ is split over k, and α lies in the kernel of γ. $\square$

The same argument applies to the Selmer group of the Jacobian J_d of the hyperelliptic curve $dy^2 = f(x)$, for any class $d \in k^*/k^{*2}$. Since the 2-Selmer groups of the twisted curves are known to become arbitrarily large (cf. [5] for the case of genus $n = 1$), the number of k-rational orbits is infinite.

8 More general representations

The three representations V of $\mathrm{SO}(W)$ that we have studied illustrate various phenomena which occur in many other cases. For the standard representation, we have seen that the invariant polynomial q_2 distinguishes the orbits with $\Delta \neq 0$ over any field k. Here the arithmetic invariant theory is the same as the geometric invariant theory.

This pleasant situation also occurs for orbits where the stabilizer G_v is trivial! An interesting example for the odd orthogonal group $\mathrm{SO}(W)$ is the reducible representation $V = W \oplus \wedge^2(W)$. This occurs as the restriction of the adjoint representation of the split even orthogonal group of the space $W \oplus \langle -1 \rangle$. In this representation, the vector $v = (w, T)$ is stable if and only if the $2n+1$ vectors $\{w, T(w), T^2(w), \ldots, T^{2n}(w)\}$ form a basis of W, or equivalently, if the invariant polynomial $\Delta(v) = \det(\langle T^i(w), T^j(w) \rangle)$ is non-zero. In this case $G_v = 1$.

One complication in this case is that the k-orbits do not cover the k-rational points of the categorical quotient: the map on points

$$V(k)/\mathrm{SO}(W)(k) \to (V/\mathrm{SO}(W))(k)$$

is not surjective. This situation is far more typical in invariant theory than the surjectivity for the three representations we studied. Another atypical property of the three (faithful) representations we studied was that a generic vector had a nontrivial stabilizer. For a generic v in a typical faithful representation V of a reductive group G, the stabilizer G_v is trivial. For G a torus and k complex, G_v is always the kernel of the representation; meanwhile, for G simple, there are only finitely many exceptions (see [20, p. 229–235]).

The adjoint representations $V = \mathfrak{g}$ of split reductive groups G generalize the second representation $V = \wedge^2(W) = \mathfrak{so}(W)$. Here the invariant polynomials correspond to the invariants for the Weyl group on a Cartan subalgebra, and generate a polynomial ring of dimension equal to the rank of G. The orbits where the discriminant Δ is non-zero correspond to the regular semi-simple elements in $\mathfrak{g}$, and the stabilizer G_v of such an orbit is a maximal torus in G. As an example, one can take the adjoint representation $V = \mathrm{Sym}^2(W)$ of the adjoint form $\mathrm{PGSp}(W) = \mathrm{PGSp}_{2n}$ of the symplectic group, where the degrees of the invariants are $2, 4, 6, \ldots, 2n$. [3, Ch 8, §13.3, VI]. For some applications to knot theory, see [15].

The representations which occur in Vinberg's theory for torsion automorphisms θ generalize the third representation $V = \mathrm{Sym}^2(W)$. Here the invariants again form a polynomial ring. As an example, one can take the reducible representation $\wedge^2(W)$ of the group $\mathrm{PGSp}(W) = \mathrm{PGSp}_{2n}$, which corresponds to the pinned outer involution θ of PGL_{2n}. When θ lifts a regular elliptic class in the Weyl group, the orbits where the discriminant Δ is non-zero are stable, and the stabilizer G_v is a finite commutative group scheme over k. Several examples of this type were discussed in [8] and [1].

9 Integral orbits

In order to develop a truly complete arithmetic invariant theory, we should consider orbits in representations not just over a field, but over $\mathbb{Z}$ or a general ring. The descent from an algebraically closed field to a general field that we have discussed in Sections 2–8 gives an indication of some of the issues that arise over more general rings, and it serves as a useful guide for the more general integral theory. In particular, just as a single orbit over an algebraically closed field can split into several orbits over a subfield, an orbit over say the field $\mathbb{Q}$ of rational numbers may then split into several orbits over $\mathbb{Z}$.

Often some of the most interesting arithmetic occurs in the passage from $\mathbb{Q}$ to $\mathbb{Z}$. For example, consider the classical representation given by the action of SL_2 on binary quadratic forms $\mathrm{Sym}_2(2)$. As we have already noted, an orbit over $\mathbb{Q}$ (as over any field) is completely determined by the value of the discriminant d of the binary quadratic forms in that orbit. However, the set of primitive integral orbits inside the rational orbit of discriminant $d \in \mathbb{Z}$ does not necessarily consist of one element, but rather is in bijection with the set of (oriented) ideal classes of the quadratic order $\mathbb{Z}[(d+\sqrt{d})/2]$ in the quadratic field $\mathbb{Q}(\sqrt{d})$ (see, e.g., [6]).

In general, to discuss integral orbits we must fix an integral model of the representation being considered. We give some canonical integral models for the three representations we have studied. For the first representation, we take W to be the odd unimodular lattice of signature $(n+1, n)$ defined by (2). Because this lattice is self-dual, we can define the adjoint of an endomorphism of W over $\mathbb{Z}$. The group G is then the subgroup of $\mathrm{GL}(W)$ consisting of those transformations g such that $gg^* = 1$ and $\det(g) = 1$. This defines a group that is smooth over $\mathbb{Z}[1/2]$ but is not smooth over $\mathbb{Z}_2$. For the other representations of G, we define $\wedge_2(W)$ as the lattice of skew self-adjoint endomorphisms of W equipped with the action of G by conjugation; we similarly define $\mathrm{Sym}_2(W)$ to be the lattice of

self-adjoint endomorphisms of W. Our objective is to describe the orbits of G on each of these three G-modules, or at least those orbits where the discriminant invariant is nonzero.

For the standard representation W, we have already seen that there is a unique orbit over $\mathbb{Q}$ for each value of the discriminant $d \in \mathbb{Q}^*$. An invariant of a $\mathbb{Z}$-orbit of a vector w in the lattice W with $\langle w, w\rangle = d$ is the isomorphism class of the orthogonal complement $U = (\mathbb{Z}w)^\perp$, which is a lattice of rank $2n$ and discriminant d over $\mathbb{Z}$. Although W is an odd lattice, the lattice U can be either even or odd. For example, when $n = 3$, the orthogonal complement U of a primitive vector w is an even bilinear space of rank 2 and discriminant d (so corresponds to an integral binary quadratic form of discriminant d) if and only if the vector w has the form $w = ae + bv + cf$ with a and c even and b odd. In this case $d = b^2 + 2ac \equiv 1$ modulo 8, and the orbits of $G(\mathbb{Z})$ on such vectors form a principal homogeneous space for the ideal class group of the quadratic order $\mathbb{Z}[(d + \sqrt{d})/2]$ of discriminant d. We note that these are precisely the quadratic orders where the prime 2 is split. In this case the group $G(\mathbb{Z})$ is isomorphic to the normalizer $N(\Gamma_0(2))$ of $\Gamma_0(2)$ in $\mathrm{PSL}_2(\mathbb{R})$, and the orbits described above correspond to the Heegner points of odd discriminant on the modular curve $X_0(2)^+$ [9, §1].

We consider next the second representation $V = \wedge_2(W)$. Here, we find that the integral orbits of $\mathrm{SO}(M)$ on the self-adjoint transformations $T : M \to M$ with (separable) characteristic polynomial $f(x) = xg(x^2) \in \mathbb{Z}[x]$ correspond to data which generalize the notion of a "minus ideal class" for the ring $R = \mathbb{Z}[x]/(f(x))$. More precisely, the ring R in $L = \mathbb{Q}[x]/(f(x))$ has an involution τ sending β to $-\beta$, where β denotes the image of x in R. Let us consider pairs (I, α), where I is a fractional ideal for R, the element α is in the $\mathbb{Q}$-subalgebra F of L fixed by τ, the product II^τ is contained in the principal ideal (α), and $N(I)N(I^\tau) = N(\alpha)$. Such a pair (I, α) gives I the structure of an integral lattice having rank $2n + 1$ and determinant $(-1)^n$, where the symmetric bilinear form on I is defined by

$$\langle x, y\rangle := \text{coefficient of } \beta^{2n} \text{ in } (-1)^n \alpha^{-1} x y^\tau. \tag{9}$$

The pair (I', α') gives an isometric lattice if $I' = cI$ and $\alpha' = cc^\tau\alpha$ for some element $c \in L^*$. The operator $S : I \to I$ defined by $S(x) = \beta x$ is skew self-adjoint, and has characteristic polynomial $f(x)$. If the integral lattice determined by the pair (I, α) has signature $(n + 1, n)$ over $\mathbb{R}$, there is an isometry $\theta : I \to M$ (cf. [22]), which is well-defined up to composition by an element in $\mathrm{O}(M)$. We obtain an $\mathrm{SO}(M)$-orbit of skew self-adjoint operators with characteristic polynomial $f(x)$ by taking $T = \theta S \theta^{-1}$. Conversely, since a skew self-adjoint $T : W \to W$ gives W the structure of a torsion free $\mathbb{Z}[T] = R$-module of rank one, every integral orbit arises in this manner. Thus the equivalence classes of pairs (I, α) for the ring $R = \mathbb{Z}[x]/(f(x))$, as defined above, index the finite number of integral orbits on $V = \wedge_2(W)$ with characteristic polynomial $f(x)$.

Let us now consider the third representation $V = \mathrm{Sym}_2(W)$. When $\dim(W) = 3$, the kernel of the trace map gives a lattice of rank 5, closely related to the space of binary quartic forms for PGL_2. The integral orbits in this case were studied in [2] and [25]. In general, the integral orbits of $\mathrm{SO}(M)$ on the self-adjoint transformations $T : M \to M$ with (separable) characteristic polynomial $f(x)$ correspond to data which generalize the notion of an ideal class of order 2 for the order $R = \mathbb{Z}[x]/(f(x))$ in the $\mathbb{Q}$-algebra $L = \mathbb{Q}[x]/(f(x))$. More precisely, we consider pairs (I, α), where I is a fractional ideal for R, the element α lies in L^*, the square I^2 of the ideal I is contained in the principal ideal (α), and the square of the norm of I satisfies $N(I)^2 = N(\alpha)$. Then the lattice I has the integral symmetric bilinear form

$$\langle x, y\rangle := \text{coefficient of } \beta^{2n} \text{ in } \alpha^{-1} x y \tag{10}$$

of determinant $(-1)^n$, and self-adjoint operator given by multiplication by β, where β again denotes

the image of x in R. The pair (I', α') gives an isometric lattice if $I' = cI$ and $\alpha' = c^2\alpha$ for some element $c \in L^*$. When this lattice has signature $(n+1, n)$ over $\mathbb{R}$, it is isometric to M and we obtain an integral orbit with characteristic polynomial $f(x)$. Conversely, since a self-adjoint $T : W \to W$ gives W the structure of a torsion free $\mathbb{Z}[T] = R$-module of rank one, every integral orbit arises in this way. Thus pairs (I, α) for the ring $R = \mathbb{Z}[x]/(f(x))$, up to the equivalence relation defined by c in L^*, index the finite number of integral orbits on $V = \mathrm{Sym}_2(W)$ with characteristic polynomial $f(x)$.

We summarize what we have established for the representations $V = \wedge_2(W)$ and $V = \mathrm{Sym}_2(W)$.

Proposition 9 *Let V denote either the representation $\wedge_2(W)$ or $\mathrm{Sym}_2(W)$ of G. Let $f(x)$ be a polynomial of degree $2n+1$ with coefficients in $\mathbb{Z}$ and non-zero discriminant in $\mathbb{Q}$; if $V = \wedge_2(W)$ we further assume that $f(x) = xg(x^2)$ for an integral polynomial g. Then the integral orbits of $G(\mathbb{Z})$ on $V(\mathbb{Z})$ with characteristic polynomial $f(x)$ are in bijection with the equivalence classes of pairs (I, α) for the order $R = \mathbb{Z}[x]/(f(x))$ defined above, with the property that the bilinear form $\langle\ ,\ \rangle$ on I (given by (9) or (10), respectively) is split.*

In terms of Proposition 4, the integral orbit corresponding to the pair (I, α) maps to the rational orbit of $\mathrm{SO}(W)(\mathbb{Q})$ on $V(\mathbb{Q})$ corresponding to the class of $\alpha \equiv \alpha^{-1}$. Here we view α as an element of (K^*/NE^*) when $V = \wedge_2(W)$, so $L = E + \mathbb{Q}$ and $L^\tau = K + \mathbb{Q}$. When $V = \mathrm{Sym}_2(W)$, we view α as an element of $(L^*/L^{*2})_{N\equiv 1}$.

Finally, we remark that it would be interesting and useful to develop a theory of cohomology that allows one to describe orbits over the integers as we have in the cases above. For example, let us consider again the representation V of the group $G = \mathrm{PGL}_2$ over $\mathbb{Q}$ given by conjugation on the 2×2 matrices v of trace zero. Then this is the adjoint representation, and is also the standard representation of $\mathrm{SO}_3 \cong \mathrm{PGL}_2$. The ring of invariant polynomials on V is generated by $q(v) := -\det(v)$, and the stabilizer G_v of a vector with $q(v) = d \neq 0$ is isomorphic to the one-dimensional torus over $\mathbb{Q}$ which is split by $K = \mathbb{Q}(\sqrt{d})$, and all vectors w with $q(w) = q(v) \neq 0$ lie in the same $G(\mathbb{Q})$-orbit.

A natural integral model of this representation is given by the action of the $\mathbb{Z}$-group $G = \mathrm{PGL}_2$ on the finite free $\mathbb{Z}$-module of binary quadratic forms $ax^2 + bxy + cy^2$. This is equivalent to the representation by conjugation on the matrices of trace zero in the subring $\mathbb{Z} + 2\mathcal{R}$ of the ring $\mathcal{R}$ of 2×2 integral matrices. In this model, the invariant polynomial is just the discriminant $d = b^2 - 4ac$ of the binary form. The content $e = \gcd(a, b, c)$ is also an invariant of a non-zero integral orbit.

We may calculate the $G(\mathbb{Z})$-orbits on the set S of forms with discriminant $d \in \mathbb{Z} - \{0\}$ and content $e = 1$ (so the binary quadratic form is primitive) via cohomology. Let $O = O(d)$ be the quadratic order of discriminant d. Then the stabilizer G_v of such an orbit in PGL_2 is a smooth group scheme over $\mathbb{Z}$ which lies in an exact sequence (in the étale topology)

$$1 \to \mathbb{G}_m \to \mathrm{Res}_{O/\mathbb{Z}}\, \mathbb{G}_m \to G_v \to 1.$$

Furthermore, the $\mathbb{Z}$-points of the quotient scheme G/G_v can be identified with the set S. Hence the orbits in question are in bijection with the kernel of the map $\gamma : H^1(\mathbb{Z}, G_v) \to H^1(\mathbb{Z}, \mathrm{PGL}_2)$ in étale cohomology. Since $H^1(\mathbb{Z}, \mathrm{PGL}_2) = 1$, the orbits are in bijection with the elements of $H^1(\mathbb{Z}, G_v)$. Since $H^1(\mathbb{Z}, \mathbb{G}_m) = H^2(\mathbb{Z}, \mathbb{G}_m) = 1$ the long exact sequence in cohomology gives

$$H^1(\mathbb{Z}, G_v) = H^1(\mathbb{Z}, \mathrm{Res}_{O/\mathbb{Z}}\, \mathbb{G}_m) = \mathrm{Pic}(O).$$

Hence the orbits of $\mathrm{PGL}_2(\mathbb{Z})$ on the set S of binary quadratic forms of discriminant $d \neq 0$ and content 1 form a principal homogeneous space for the finite group $\mathrm{Pic}(O(d))$ of isomorphism classes of projective $O(d)$-modules of rank one. Thus the number of primitive integral orbits contained in the rational orbit of discriminant d is given by the class number of $O(d)$.

References

[1] M. Bhargava and W. Ho, Coregular spaces and genus one curves, preprint.

[2] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, ArXiv: 1006.1002 (2010).

[3] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, 1982.

[4] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** (1963), 7–25.

[5] R. Bolling, Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gross werden, *Math. Nachr.* **67** (1975), 157–179.

[6] D. A. Buell, *Binary quadratic forms: classical theory and modern computations*, Springer-Verlag, 1989.

[7] R. Donagi, Group law on the intersection of two quadrics, *Annali della Scuola Normale Superiore di Pisa* **7** (1980), 217–239.

[8] B. Gross, On Bhargava's representations and Vinberg's invariant theory, In: *Frontiers of Mathematical Sciences*, International Press (2011), 317–321.

[9] B. Gross, W. Kohnen, and D. Zagier, Heegner points and derivatives of L-series II, *Math. Ann.* **278** (1987), 497–562.

[10] R. Kottwitz, Stable trace formula: cuspidal tempered terms, *Duke Math. J.* **51** (1984), 611–650.

[11] A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, AMS Colloquium Publications **44**, 1998.

[12] A. Kostrikin and P. H. Tiep, *Orthogonal decompositions and integral lattices*, deGruyter Expositions in Mathematics **15**, Berlin, 1994.

[13] R. Langlands, Stable conjugacy—definitions and lemmas, *Canadian J. Math* **31** (1979), 700–725.

[14] R. Langlands, Les débuts d'une formule des traces stable, *Publ. Math. de L'Univ. Paris VII*, **13**, 1983.

[15] A. Miller, Knots and arithmetic invariant theory, preprint.

[16] J. Milnor and D. Husemoller, *Symmetric bilinear forms*, Springer Ergebnisse **73**, 1970.

[17] D. Mumford, J. Fogarty, F. Kirwan *Geometric invariant theory*, Springer Ergebnisse **34**, 1994.

[18] D. Panyushev, On invariant theory of θ-groups, *J. Algebra* **283** (2005), 655–670.

[19] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, *Pure and Applied Mathematics* **139**, Academic Press, Inc., Boston, MA, 1994.

[20] V. L. Popov and E. B. Vinberg, *Invariant Theory*, in *Algebraic Geometry IV*, Encylopaedia of Mathematical Sciences **55**, Springer-Verlag, 1994.

[21] J-P. Serre, *Galois cohomology*, Springer Monographs in Mathematics, 2002.

[22] J-P. Serre, *A course in arithmetic*, Springer GTM **7**, (1978).

[23] D. Shelstad Orbital integrals and a family of groups attached to a real reductive group, *Ann. Sci. École Norm. Sup.* **12** (1979), 1–31.

[24] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, *Acta Arith* **98** (2001), 245–277.

[25] M. Wood, *Moduli spaces for rings and ideals*, Ph.D. thesis, Princeton University, 2008.