University of Waterloo

MMath Research Paper

Arithmetic Invariant Theory: An Overview

Andrej Vuković

supervised by
Prof. Xiaoheng Jerry Wang

September 16, 2019

Contents

Abstract

We give an overview of arithmetic invariant theory (AIT), covering numerous examples from the papers [1] and [2] of Bhargava, Gross, and Wang. We include background material that is not in the original papers but that is useful to have in one place. We discuss some new research directions, including an approach due to Auel, Geraschenko, and Zureick–Brown ([3]) for AIT over schemes.

1 Introduction

"The theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head." —Hermann Weyl ([34])

1.1 History of invariant theory

Much of the history described in this section may be found in [10].

Although the first inklings of invariant theory were already apparent in the late eighteenth century study of binary quadratic forms by Gauss and other number theorists, invariant theory emerged as an independent discipline only in the nineteenth century as algebraic geometers began to recognize the advantages of working in affine projective space. Given a curve defined by homogeneous polynomial equations in affine projective space, the "affine" condition means that there is no fixed origin, and the "projective" condition means that equations are defined up to rescaling the variables by a non-zero scalar. It is therefore profitable to study how homogeneous polynomials change when their variables are rescaled by the composition of a translation and a dilation, i.e., by an affine transformation.
In the two-variable case, this reduces to the following problem. Let

$$f(x,y) = f_0x^n + f_1x^{n-1}y + ... + f_ny^n$$

be a binary n-ic form with coefficients in some field k, usually taken to be algebraically closed. In the rest of this subsection, we will take $k = \mathbb{C}$. The group $\mathrm{SL}_2(\mathbb{C})$ of 2×2 matrices with complex entries and determinant 1 acts on such forms on the left by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(x,y) = f(ax+by, cx+dy).$$

Now, suppose $g(f_0, ..., f_n)$ is a polynomial in the coefficients of $f(x,y)$. Then $\mathrm{SL}_2(\mathbb{C})$ also acts on g as follows.

(i) Given

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}),$$

calculate $f(ax+by, cx+dy)$. Note that $f(ax+by, cx+dy)$ will have no terms of higher degree than n since we have only made linear substitutions. Let f_i' be the coefficient of $x^{n-i}y^i$ in

$f(ax+by, cx+dy)$.

(ii) Then the $\mathrm{SL}_2(\mathbb{C})$-action on $f(x,y)$ induces an action on the coefficient f_i by sending it to f_i', defined as above. This action extends to any polynomial in the f_i by sending the polynomial $g(f_0, ..., f_n)$ to $g(f_0', ..., f_n')$.

Definition 1.1. An *invariant of the binary n-ic form*

$$f(x,y) = f_0x^n + f_1x^{n-1}y + ... + f_ny^n$$

over $\mathbb{C}$ is a polynomial $g(f_0, ..., f_n)$ in its coefficients that is invariant under the $\mathrm{SL}_n(\mathbb{C})$-action just described.

Mathematicians set out to compute invariants. A general technique for doing so, known as the *symbolic method*, was developed by Arthur Cayley and others in the middle of the nineteenth century. However, the technique was not entirely rigorous and quite unwieldy.

The next observation made by nineteenth century mathematicians was that the invariant polynomials form an algebra. They then investigated whether one could find finitely many generators for the algebra of invariants. This search was put to an end in 1890 when Hilbert ([15]) proved, using what was essentially an argument in commutative algebra, that all such algebras are finitely-generated.

Invariant theory lay dormant between the 1890s and the 1930s. It was revived by the work of Hermann Weyl, Issai Schur, Elie Cartan, and others. These mathematicians discovered that invariant theory had a natural interpretation within the representation theory of matrix groups. In this language, invariant theory is the study of a group G acting on a representation V over an algebraically closed field k. The ring of polynomials on V is denoted $k[V]$. The G-action on V induces a G-action on $k[V]$ as above.

The algebra of polynomials invariant under this G-action is then a k-subalgebra $k[V]^G$ of $k[V]$.

In the late 1950s, Alexander Grothendieck and his associates reformulated algebraic geometry using the definition of a "scheme", a generalization of a system of polynomial equations. The theory of matrix groups was then subsumed into the theory of reductive group schemes. David Mumford, inspired by moduli problems, developed the field of geometric invariant theory (GIT) in his landmark book [24]. Building on work of Chevalley, Tate, and others, Mumford reformulated invariant theory in the scheme-theoretic language.

However, work in GIT generally assumed the base field to be separably closed. Arithmetic invariant theory, introduced by Bhargava, Gross, and Wang in [1] and [2], is the area that studies what occurs over a base field that is not necessarily separably closed. In particular, the foundational question of AIT is as follows. Let G be a reductive group scheme with a representation V over a field k. How can we characterize the $G(k)$-orbits lying within a given

$G(k^s)$-orbit? This is the question that we will discuss in the sections to come.

In Section 2, we discuss assorted background material necessary to understand the content of subsequent sections. In Section 3, we discuss AIT over fields and give a number of illustrative examples from [1]. In Section 4, we discuss obstructions, in AIT over fields, to lifting rational points of the categorical quotient to rational orbits with many examples from [2]. In Section 5, we discuss new developments in AIT over schemes, with a particular focus on $\mathbb{Z}$. In the Appendix, we discuss non-abelian Galois cohomology in the context of AIT.

2 Background

We assume quite a lot of background in modern algebraic geometry. The reader should know what "sheaves" and "schemes" are and should be familiar with some basic scheme-theoretic constructions (e.g., fibred products). A good reference for that material is [11]. We will not develop the theory of group schemes here, opting instead merely to review the definitions. Good references for the theories of algebraic groups, affine group schemes, and reductive groups are [18], [19], and [20], respectively. The definitions and examples in this section can be found (possibly with some minor modifications) in any standard source on those subjects. Although we will review topics from étale and flat cohomology, familiarity with the basic notions (e.g., knowing when a morphism is étale or flat) is assumed. Good references for this material are [22] and [23]. We also assume some familiarity with categorical quotients, which are discussed in [24].

2.1 Group schemes

Definition 2.1. [24] Let S be a scheme. A *group scheme* over S is a group object in the category of S-schemes. More precisely, it consists of the following data:

(i) A scheme G over S with structure morphism $\pi : G \to S$.

(ii) Morphisms of S-schemes $\mu : G \times_S G \to G$ (corresponding to multiplication), $\iota : G \to G$ (corresponding to taking inverses), and $e : S \to G$ (corresponding to the group identity) satisfying the following three conditions:

(a) (Associativity.) The following diagram commutes:

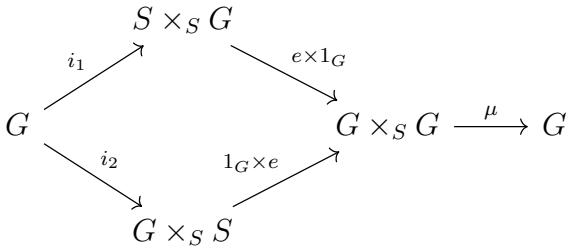
$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{1_G \times \mu} & G \times_S G \\ \downarrow{\scriptstyle \mu \times 1_G} & & \downarrow{\scriptstyle \mu} \\ G \times_S G & \xrightarrow{\mu} & G \end{array}$$

(b) (Property of inverse.) Let $\Delta : G \to G \times_S G$ be the diagonal morphism. Then both of the following compositions are equal to $e \circ \pi$:

$$G \xrightarrow{\Delta} G \times_S G \xrightarrow{1_G \times \iota} G \times_S G \xrightarrow{\mu} G$$

$$G \xrightarrow{\Delta} G \times_S G \xrightarrow{\iota \times 1_G} G \times_S G \xrightarrow{\mu} G$$

(c) (Property of identity.) Let $i_1 : G \to S \times_S G$ and $i_2 : G \to G \times_S S$ be the canonical isomorphisms. Then both compositions in the following diagram are equal to 1_G:



A *morphism* of group schemes is a morphism of schemes that is compatible with the multiplication operation.

Remark 2.2. When considering a group scheme G over $\mathrm{Spec}(k)$ for a field k, we say for convenience that G lies over k.

Definition 2.3. Let G be a group scheme over S with multiplication map μ. A *subgroup scheme* H of G over S is a subscheme H of G such that $m|_{H \times_S H}$ factors through H and induces a group scheme structure on H over S.

We generally care only about the following special type of group scheme.

Definition 2.4. An *algebraic group* is a group scheme of finite type over a field. When the underlying scheme of the algebraic group is a variety, we call it a *group variety*. When it is an affine scheme, we call it an *affine* algebraic group. Morphisms for all these objects are the corresponding morphisms in the category of group schemes.

The following useful theorem is due to Cartier.

Theorem 2.5. *Every affine algebraic group over a field k of characteristic zero is smooth.*

Proof. See Ch. III, §h. of [18]. □

Example 2.6. Let R be a unital commutative ring. The following are all examples of algebraic groups. (For proofs that they are, see [19, §3].)

(i) The *additive group scheme* $\mathbb{G}_a$ is the functor $R \mapsto (R, +)$.

(ii) The *multiplicative group scheme* $\mathbb{G}_m$ is the functor $R \mapsto (R^\times, \cdot)$.

(iii) The n^{th} *roots of unity group scheme* μ_n is given by $R \mapsto \{r \in R | r^n = 1\}$.

(iv) The *general linear group scheme* GL_n is the functor $R \mapsto \mathrm{GL}_n(R)$. More generally, given a k–vector space V, we define GL_V to be the functor $R \mapsto \mathrm{Aut}_R(V \otimes_k R)$ (i.e., the group of R-linear automorphisms of V).

(v) All the usual matrix groups can be viewed as algebraic groups. In particular, there is a *special linear group scheme* SL_n, an *orthogonal group scheme* O_n, a *special orthogonal group scheme* SO_n, a *projective general linear group scheme* PGL_n, a *symplectic group scheme* Sp_{2n}, and so on.

Definition 2.7. Let G be a group scheme over a scheme S. A *representation* of G on a finite-dimensional vector space V is a natural transformation of functors $G \to \mathrm{GL}_V$ that is a homomorphism on the underlying groups. In particular, if G is defined over a field k, then a representation ρ includes the data of a homomorphism $\rho(R) : G(R) \to \mathrm{GL}_V(R)$ for every k-algebra R. A representation ρ over a field k is said to be *faithful* if $\rho(R)$ is injective for every k-algebra R.

Definition 2.8. An algebraic group G over a field k is said to be *linear* if it has a faithful finite-dimensional representation $G \to \mathrm{GL}_V$. Fix such a representation $j : G \to \mathrm{GL}_V$. An element $g \in G(k)$ is said to be *semisimple* if $j(g)$ is diagonalizable (i.e., semisimple as a linear map) and *unipotent* if $j(g)$ is unipotent as a linear map.

Remark 2.9. [5] Since we require the representation j to be faithful, the properties of semisimplicity and unipotence are independent of the particular choice of j. By the theory of Jordan decomposition, if G is an algebraic group over a field k, then for any $g \in G(k)$, there exist unique commuting elements $g_{ss}, g_u \in G(k)$ such that $g = g_{ss}g_u$. These are known as the *semisimple part* and the *unipotent part* of g, respectively, and their product is the *Jordan decomposition* of g. Semisimplicity, unipotence, and Jordan decompositions are preserved under homomorphisms of linear algebraic groups.

Definition 2.10. A linear algebraic group G over a field k is *unipotent* if for every $g \in G(k)$, g is equal to the unipotent part g_u of its Jordan decomposition.

Example 2.11. [5] Over a field k, the group scheme $\mathbb{G}_a$ is unipotent via the faithful representation $\mathbb{G}_a \to \mathrm{GL}_2$ given by $x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ since each such matrix is unipotent.

Definition 2.12. Let G be a linear algebraic group over a field k. We say G is *reductive* if it contains no non-trivial unipotent normal connected linear algebraic k-subgroup.

Definition 2.13. Let G be a smooth group scheme $G \to S$ where S is a base scheme and G is affine over S. Let p be a geometric point of S so that the residue field $k(p)$ is separably closed. Let $G_{k(p)} = G \times_S \mathrm{Spec}(k(p))$ be the geometric fibre. Suppose that for every geometric point p of S, the fibre $G_{k(p)}$ is a connected reductive group. Then we say that G is *reductive* over S.

Example 2.14. The group schemes GL_n, SL_n, SO_n, and Sp_{2n} are reductive for all $n \in \mathbb{N}$ over any field k. In particular, $\mathbb{G}_m = \mathrm{GL}_1$ is reductive. However, $\mathbb{G}_a$ is not reductive. We defer the proofs of these claims to [5] and [20], particularly §17 of the latter.

2.2 Cohomology

Let k be a field and G a group scheme. Let V be a representation of G with $v \in V(k)$. Let G_v be the stabilizer of v, which is a group subscheme of G. Let k^s be a separable closure of k. We adopt the usual notation of $H^1(k, G)$ for the first Galois cohomology $H^1(\mathrm{Gal}(k^s/k), G(k^s))$ and $H^1(k, G_v)$ for $H^1(\mathrm{Gal}(k^s/k), G_v(k^s))$.

Definition 2.15. [26] Let Γ be a profinite group. A topological space X is said to be a Γ-*set* if it is discrete and is acted on continuously by Γ. (We will use the notation $g(x)$ for the image of $x \in X$ under the action of $g \in G$.) For $\sigma \in \Gamma$ and $x \in X$, we denote the image of x under σ by x^σ. Given two Γ-sets X and X', a Γ-*morphism* from X to X' is a continuous map $f : X \to X'$ that commutes with the action of Γ. A Γ-*group* X is a Γ-set with a group structure such that for all $x, y \in X$ and all $\sigma \in \Gamma$,

$$(xy)^\sigma = x^\sigma y^\sigma.$$

Definition 2.16. [25] If X is a Γ-set and it is additionally equipped with the structure of a module, and if this structure is compatible with the Γ-action, we call X a Γ-*module*. When Γ is a Galois group and X is a Γ-module, we say it is a *Galois module*.

Lemma 2.17. *[26] Let Γ be a profinite group, and let X be a Γ-set. For every $x \in X$, the stabilizer of x under the Γ-action is open.*

Proof. Let $x \in X$. Since X is discrete and the action is continuous, preimages along the map $G \times X$ given by $(g, x) \mapsto x$ are open, so the set of (g, x) for which $g(x) = x$ is open. Since the projection onto the first coordinate is an open map, the set of $g \in G$ for which $g(x) = x$ is also open. In other words, the stabilizer of x is open for every $x \in X$. □

Definition 2.18. [26] Let Γ be a profinite group and X a Γ-group. A 1-*cocycle* with values in X is a continuous map $\Gamma \to X$ given by $\sigma \mapsto a_\sigma$ such that for all $\sigma, \tau \in \Gamma$,

$$a_{\sigma\tau} = a_\sigma a_\tau^\sigma.$$

Note that since X is equipped with the discrete topology, the continuity of a 1-cocycle is equivalent to openness of preimages along the map $\sigma \mapsto a_\sigma$. We denote the set of 1-cocycles by $Z^1(\Gamma, X)$. Two 1-cocycles a and b are said to be *cohomologous* if there exists $c \in X$ such that for all $\sigma \in \Gamma$,

$$b_\sigma = c^{-1} a_\sigma c^\sigma.$$

Being cohomologous defines an equivalence relation $\sim_{\mathrm{coho},1}$ on $Z^1(\Gamma, X)$.

Definition 2.19. The cohomology theory defined so far is known as *(continuous) profinite group cohomology*. Standard group cohomology is defined similarly without the requirement that the group Γ be profinite. There is also a version of group cohomology in which the cocycles are not required to be continuous, which can change some calculations. In the particular case where $\Gamma = \mathrm{Gal}(k^s/k)$ for some field k with separable closure k^s, we refer to the resulting cohomology theory as *Galois cohomology*.

With these notions at hand, we are ready to define the first two non-abelian cohomology groups of Γ and X.

Definition 2.20. [26] Let Γ be a profinite group and X a Γ-set. Define

$$H^0(\Gamma, X) = X^\Gamma,$$

the set of elements of X fixed by the Γ-action. If X is a Γ-group, the group structure on X induces a group structure on $H^0(\Gamma, X)$.

Suppose now that X is a Γ-group. Define

$$H^1(\Gamma, X) = Z^1(\Gamma, X)/\sim_{\text{coho},1} .$$

Note that the set $H^1(\Gamma, X)$ has a unit element, denoted 1, which is the equivalence class of the constant cocycle given by sending each $\sigma \in \Gamma$ to the identity of X. This will allow us to define exact sequences in Galois cohomology.

Defining the second non-abelian Galois cohomology set is more difficult; we include a description in the appendix.

Every cohomology theory obeying the Eilenberg–Steenrod axioms has the property that, given a short exact sequence (in the correct category for that theory), there is a corresponding long exact sequence in cohomology. Since many objects in algebraic geometry and algebraic number theory fit into short exact sequences, it is useful to know how to compute certain basic cohomology sets and groups in order to compute the rest using long exact sequences in cohomology. The next few results show us a few such computations.

A famous theorem from the late 1800s, known as "Hilbert's Theorem 90", has taken on a life of its own. Many generalizations and variants of the original theorem are casually referred to by the same name. We now state what could be described as a *generalization of Hilbert's Theorem 90* written in the language of Galois cohomology.

Theorem 2.21. *[26] Let L/K be a Galois field extension with $G = Gal(L/K)$. Let $n \in \mathbb{N}$, and let H be either $GL_n(L)$ or $SL_n(L)$. Then $H^1(G, H)$ is trivial. Moreover, $H^1(G, L)$ is trivial. (In fact, part of this theorem can be generalized further to a result in étale cohomology, which we discuss later.)*

The next result will let us perform more computations. We will show that two classical areas of number theory (*Kummer theory* and *Artin–Schreier theory*) are its consequences. The proof we give is similar to the one on p. 91 of [4]. Note that the statement concerns profinite group cohomology.

Proposition 2.22. *Let G be a profinite group, and let A be a G-module. Suppose we have a surjective G-module homomorphism $\pi : A \to A$. Suppose that G acts trivially on $C = \ker(\pi)$ and that $H^1(G, A)$ is trivial. Then, letting A^G denote the G-fixed points of A, we have that*

$$A^G/\pi(A^G) \simeq Hom(G, C).$$

Proof. Consider the short exact sequence

$$0 \longrightarrow C \hookrightarrow A \xrightarrow{\pi} A \longrightarrow 0$$

Since G acts trivially on C, $C^G = C$ and $H^1(G, C) = \mathrm{Hom}(G, C)$. Since $H^1(G, A)$ is trivial by assumption, by applying the long exact sequence in group cohomology, we obtain

$$0 \longrightarrow C \longrightarrow A^G \xrightarrow{\pi} A^G \longrightarrow \mathrm{Hom}(G, C) \longrightarrow 0$$

and from exactness it follows that $A^G/\pi(A^G) \simeq \mathrm{Hom}(G, C)$, as claimed. □

Kummer theory is a type of Galois theory that involves the adjunction of roots of unity to a base field. We now show that it is a corollary of the previous proposition. First, we define the type of field extension with which we are concerned in this setting.

Definition 2.23. A *Kummer extension* is a Galois extension L/K such that K contains n distinct n^{th} roots of unity for some fixed $n \in \mathbb{N}$ and such that $\mathrm{Gal}(L/K)$ is abelian of exponent n (i.e., the least common multiple of the orders of its elements is n).

Now we recover the main result in Kummer theory.

Corollary 2.24. *Let k be a field with a choice of separable closure k^s. Suppose k contains the group μ_n of n^{th} roots of unity. (Note that this implies $char(k) \nmid n$.) Then*

$$k^\times/(k^\times)^n \simeq Hom(Gal(k^s/k), \mu_n) \simeq H^1(Gal(k^s/k), \mu_n).$$

In particular, cyclic extensions of k of exponent dividing n are of the form $k(\sqrt[n]{a})/k$ for some $a \in k^\times$.

Proof. In the notation of Proposition 2.22, let $G = \mathrm{Gal}(k^s/k)$ be equipped with the profinite topology. Let $A = (k^s)^\times$, and let $\pi(x) = x^n$ for some fixed $n \in \mathbb{N}$. Then $C = \ker(\pi)$ consists of n^{th} roots of unity contained in $(k^s)^\times$, which by assumption all lie in $k^\times$, so $C \simeq \mu_n$ and G acts trivially on C. Moreover, $H^1(G, A) = H^1(\mathrm{Gal}(k^s/k), (k^s)^\times)$ is trivial by Theorem 2.21 applied to GL_1. By Proposition 2.22,

$$A^G/\pi(A^G) \simeq \mathrm{Hom}(G, C),$$

that is,

$$k^\times/(k^\times)^n \simeq \mathrm{Hom}(\mathrm{Gal}(k^s/k), \mu_n).$$

More explicitly, this isomorphism is given by $a \mapsto (\sigma \mapsto (\sqrt[n]{a})^\sigma/\sqrt[n]{a})$. Suppose now that L/k is a cyclic extension of exponent dividing n. Fix an embedding $\mathrm{Gal}(L/k) \hookrightarrow \mu_n$. Composing it with a quotient map in Galois groups gives a group homomorphism $\mathrm{Gal}(k^s/k) \to \mu_n$. Let φ denote this map. By the isomorphism we obtained, we know that there exists $a \in k^\times$ such that $\varphi(\sigma) = (\sqrt[n]{a})^\sigma/\sqrt[n]{a}$. Then $\ker(\varphi)$ is the subgroup of $\mathrm{Gal}(k^s/k)$ with fixed field $k(\sqrt[n]{a})$. Since φ factors through an embedding of $\mathrm{Gal}(L/k)$ into μ_n, it follows that $L \simeq k(\sqrt[n]{a})$ for some $a \in k^\times$. □

Artin–Schreier theory is the analogue of Kummer theory for fields of positive characteristic. We can recover its main result as well.

Corollary 2.25. *Let k be a field, and let k^s be a separable closure of k. Suppose $char(k) = p$. Let $\pi : k^s \to k^s$ be defined by $\pi(x) = x^p - x$. Then*

$$k/\pi(k) \simeq Hom(Gal(k^s/k), \mathbb{Z}/p\mathbb{Z}) \simeq H^1(Gal(k^s/k), \mathbb{Z}/p\mathbb{Z}).$$

In particular, $\mathbb{Z}/p\mathbb{Z}$-extensions of k are of the form $k[x]/(x^p - x - a)$ over k for some $a \in k$.

Proof. In the notation of Proposition 2.22, let $G = \mathrm{Gal}(k^s/k)$ be equipped with the discrete topology. Let $A = (k^s, +)$ be the additive group of k^s. Then, since $x^p - x - a$ is separable for every $a \in A$, π is surjective on A. Also,

$$C = \ker(\pi) \simeq \mathbb{F}_p$$

is a copy of the prime field $\mathbb{F}_p$ inside K. In particular, G acts trivially on C. Moreover, $H^1(G, A) = H^1(\mathrm{Gal}(k^s/k), A)$ is trivial by Theorem 2.21. By Proposition 2.22,

$$A^G/\pi(A^G) \simeq \mathrm{Hom}(G, C),$$

that is,

$$k/\pi(k) \simeq \mathrm{Hom}(\mathrm{Gal}(k^s/k), \mathbb{Z}/p\mathbb{Z}).$$

The form of $\mathbb{Z}/p\mathbb{Z}$-extensions of k follows by the same sort of argument as in the proof of the previous corollary. □

Remark 2.26. Note that although there is a unique group of prime order up to isomorphism, μ_p and $\mathbb{Z}/p\mathbb{Z}$, viewed as a group schemes over a field K, generally have different Galois modules structures. These structures coincide precisely when K contains μ_p so that μ_p is fixed under the Galois action. As group schemes over a field, μ_p and $\mathbb{Z}/p\mathbb{Z}$ are also not isomorphic in general.

Later in the paper, when doing some Galois cohomology calculations, we will use the following standard terminology.

Definition 2.27. Let k be a field with a choice of separable closure k^s. The Galois cohomology group $H^2(\mathrm{Gal}(k^s/k), \mathbb{G}_m(k^s))$ is known as the *Brauer group* of k and is denoted $\mathrm{Br}(k)$.

Finally, we summarize some facts about étale cohomology without giving proofs. Recall that étale cohomology is a *Weil cohomology theory* and therefore satisfies all the usual properties we would expect from a well-behaved cohomology theory (e.g., Poincaré duality, Künneth isomorphism, versions of the Eilenberg–Steenrod axioms). Étale cohomology can be thought of as an analogue of Galois cohomology over an arbitrary base scheme. The following result makes this precise.

Proposition 2.28. *[28] Let k be a field with separable closure k^s. Let $G = Gal(k^s/k)$. Let M be a G-module equipped with the discrete topology. Let $\mathcal{M}$ be the sheaf associated to M. Then for all $n \geq 1$,*

$$H^n_{cont}(G, M) \simeq H^n_{\acute{e}t}(Spec(k), \mathcal{M})$$

where the left-hand side is continuous Galois cohomology and the right-hand side is étale cohomology.

Proof. See §2.4 of [28]. □

We now summarize certain calculations in étale cohomology that we will use later.

Proposition 2.29. *[22], [16] (i) (Hilbert's Theorem 90 for étale cohomology). Let X be a scheme. Then $H^1_{ét}(X, \mathbb{G}_m) = Pic(X)$.*

(ii) Let K be a number field with ring of integers O_K. Let $X = Spec(O_K)$. Then

$$H^i_{ét}(X, \mathbb{G}_m) = \begin{cases} O_K^\times & i = 0 \\ \mathrm{Pic}(X) & i = 1 \\ 0 & i = 2 \\ \mathbb{Q}/\mathbb{Z} & i = 3 \\ 0 & i \geq 4 \end{cases}$$

Proof. (i) See Corollary 11.6 of [22].

(ii) See p. 538 of [16].

□

When R is a commutative ring, we will often write $H^i_{\text{ét}}(R, \mathcal{F})$ instead of $H^i_{\text{ét}}(\mathrm{Spec}(R), \mathcal{F})$.

2.3 Orthogonal spaces

Every definition, statement, and proof in this section is taken from [17], possibly with slight modifications, except where otherwise indicated.

Definition 2.30. Let R be a unital commutative ring. Let M be a left R-module. We say a map $b : M \times M \to R$ is a *bilinear form* on M if it is linear in each coordinate. If b additionally satisfies $b(x, y) = b(y, x)$ for all $x, y \in M$, we say it is *symmetric*. If b satisfies $b(x, y) = -b(y, x)$ for all $x, y \in M$, we say it is *skew-symmetric* or *anti-symmetric*. If $b(x, x) = 0$ for all $x \in M$, we say it is *alternating*. If the following two non-degeneracy conditions are satisifed, b is called an *inner product*:

(i) For each R-linear map $\phi : M \to R$, there exists a unique element $x \in M$ such that $y \mapsto b(x, y)$ is equal to ϕ.

(ii) For each R-linear map $\phi : M \to R$, there exists a unique element $y \in M$ such that $x \mapsto b(x, y)$ is equal to ϕ.

When b is symmetric or skew-symmetric, (i) and (ii) are equivalent. If M is finitely-generated and free over R and b is a symmetric bilinear form, the pair (M, b) is called an *orthogonal space*. If, in addition, b is an inner product, the orthogonal space (M, b) is said to be *non-degenerate*.

Two orthogonal spaces (X_1, b_1) and (X_2, b_2) are *isomorphic* if there exists an R-linear bijection $f : X_1 \to X_2$ such that $b_2(f(x), f(y)) = b_1(x, y)$ for all $x, y \in X_1$.

We observe that an alternating form b is necessarily skew-symmetric because for any x, y,

$$0 = b(x + y, x + y) = b(x, x) + b(x, y) + b(y, x) + b(y, y) = b(x, y) + b(y, x).$$

Conversely, any skew-symmetric form is alternating if 2 is not a zero divisor since skew-symmetry implies that $b(x, x) + b(x, x) = 0$ for any x.

Definition 2.31. Let (M, b) be an orthogonal space over the ring R. Since any two bases of a free module over a unital commutative ring have the same cardinality, M has an R-basis $\{e_1, ..., e_n\}$ for some unique $n \geq 1$. This value n is the *rank* or *dimension* of M and is equal to the rank of M as an R-module.

The $n \times n$ matrix $B = (b(e_i, e_j))_{1 \leq i,j \leq n}$ is called a *Gram matrix* of (M, b).

Lemma 2.32. *Let (M, b) be an orthogonal space where M is an R-module. The bilinear form b is an inner product if and only if the Gram matrix $B = (b(e_i, e_j))$ is invertible.*

Proof. The dual module $\mathrm{Hom}_R(M, R)$ has a dual basis, which we denote $\{e_1^*, ..., e_n^*\}$. There is a homomorphism $M \to \mathrm{Hom}_R(M, R)$ given by $x \mapsto b(x, -)$ for $x \in M$. In terms of the bases of M and $\mathrm{Hom}_R(M, R)$, this map is given by

$$e_i \mapsto \sum_{1 \leq j \leq n} b(e_i, e_j) e_j^*.$$

The non-degeneracy conditions required of an inner product then hold if and only if B is invertible. □

Definition 2.33. Given a unital commutative ring R and a matrix $B = (b_{ij}) \in M_n(R)$, the symbol $\langle B \rangle$ will denote the orthogonal space (R^n, b) with standard basis $\{e_1, ..., e_n\}$ and bilinear form b defined by $b(e_i, e_j) = b_{ij}$.

Lemma 2.34. *The orthogonal spaces $\langle B \rangle$ and $\langle B' \rangle$ are isomorphic if and only if $B' = ABA^T$ for some invertible A.*

Proof. Suppose that $\langle B \rangle \simeq \langle B' \rangle$. Then their underlying modules, being free and finitely-generated, have the same rank. Suppose $\{e_1, ..., e_n\}$ and $\{e'_1, ..., e'_n\}$ are bases for the underlying modules of $\langle B \rangle$and $\langle B' \rangle$, respectively. Then there exists some invertible matrix $A = (a_{ij})$ such that

$$e'_i = a_{i1} e_1 + ... + a_{in} e_n$$

for every $1 \leq i \leq n$. Let b be the bilinear form corresponding to B (i.e., if $B = (b_{ij})$, then $b(e_i, e_j) = b_{ij}$) and b' the bilinear form corresponding to B'. Then

$$b'(e'_i, e'_j) = \sum_{1 \leq k,l \leq n} a_{ik} b(e_k, e_l) a_{jl},$$

and it follows that $B' = ABA^T$. The converse follows by the same argument played in reverse. □

Note that if B is a Gram matrix of a non-degenerate orthogonal space (M, b), then b is an inner product, so $\det(B)$ lies in $R^\times$ by Lemma 2.32. Suppose $B' = ABA^T$ for some invertible A. Then by Lemma 2.34, $\langle B\rangle \simeq \langle B'\rangle$. Also, $\det(B') = \det(A)^2 \det(B)$. Therefore, the value of the determinant can be viewed as lying in $R^\times/R^{\times 2}$. This motivates the following definition from [17].

Definition 2.35. Given a non-degenerate orthogonal space (M, b) over a unital commutative ring R, the *determinant* of (M, b) is the element of $R^\times/R^{\times 2}$ represented by $\det(B)$, where B is any matrix with $\langle B\rangle \simeq (M, b)$. If M has dimension $2n$ or $2n + 1$ over R, then its *discriminant* is defined to be $(-1)^n$ times its determinant.

Definition 2.36. Let (M_1, b_1),..., (M_n, b_n) be orthogonal spaces over a unital commutative ring R. Their *orthogonal sum* is the orthogonal space whose underlying module is $M = M_1 \oplus ... \oplus M_n$ and whose bilinear form b is defined by

$$b(x_1 \oplus ... \oplus x_n, y_1 \oplus ... \oplus y_n) = \sum_{1\le i\le n} b_i(x_i, y_i).$$

We note that the orthogonal sum (M, b) is a non-degenerate orthogonal space if and only if each (M_i, b_i) is a non-degenerate orthogonal space. Since the M_i are all free and finitely-generated over R, the rank of M is the sum of the ranks of the M_i, and the determinant of M is the product of the determinants of the M_i.

Definition 2.37. Let $X = (M, b)$ be an orthogonal space. The *perpendicular space* of M with respect to b, denoted by $M^\perp$, consists of all $x \in M$ such that $b(x, M) = 0$, i.e., $b(x, y) = 0$ for all $y \in M$. The *perpendicular space* of X is defined to be $X^\perp = (M^\perp, b)$.

Remark 2.38. Suppose that $X = (V, b)$ is an orthogonal space over a field k (so that V is a k-vector space), b is a non-degenerate bilinear form on V, and W is a subspace of V. In this case, non-degeneracy of b reduces to the condition that if $b(v, w) = 0$ for all $w \in V$, then $v = 0$ (and similarly for the second coordinate). It follows that $b|_W$ is non-degenerate if and only if $W \cap W^\perp = \{0\}$.

Definition 2.39. Let $X = (M, b)$ be an orthogonal space over a unital commutative ring R. If $\mathrm{rank}_R(M)$ is even, we say X is *split* if there exists a free submodule $N \subseteq M$ such that N is a direct summand of M and $N = N^\perp$. If $\mathrm{rank}_R(M)$ is odd, say $\mathrm{rank}_R(M) = 2n + 1$, we say X is *split* if there exists a free submodule $N \subseteq M$ such that N is a direct summand of M and $\mathrm{rank}_R(N) = n$. In either case, such a submodule N is said to be *isotropic*.

We will encounter the next example once again in a later section.

Example 2.40. Let V be a $2n$-dimensional vector space over a field k with $\mathrm{char}(k) \neq 2$, with basis $\{e_1, ..., e_n, f_n, ..., f_1\}$, and with symmetric inner product defined by

$$\langle e_i, e_j\rangle = \langle f_i, f_j\rangle = 0, \langle e_i, f_j\rangle = \delta_{ij}.$$

Let W be a $(2n + 1)$-dimensional vector space over a field k with $\mathrm{char}(k) \neq 2$, with basis $\{e_1, ..., e_n, u, f_n, ..., f_1\}$, and with symmetric inner product defined by

$$\langle e_i, e_j\rangle = \langle f_i, f_j\rangle = \langle e_i, u\rangle = \langle f_i, u\rangle = 0, \langle e_i, f_j\rangle = \delta_{ij}, \langle u, u\rangle = 1.$$

Then V and W are both split over k with $\text{span}_k\{e_1, ..., e_n\}$ being an isotropic subspace for either.

Lemma 2.41. *Suppose (M, b) is an orthogonal space, so that in particular b is symmetric. Let N be a submodule of M, and suppose that the restriction of b to $N \times N$ is an inner product on N. Then $M \simeq N \oplus N^\perp$.*

Proof. Suppose $n \in N \cap N^\perp$. Then $b(n, n') = 0$ for all $n' \in N$, so $n = 0$, which implies $N \cap N^\perp = \{0\}$. It remains to prove that every element of M can be written as a sum of one element from N and one element from $N^\perp$.

Fix any $x \in M$. Consider the map $n' \mapsto b(x, n')$ defined on N. By the non-degeneracy conditions on inner products, there exists a unique $n \in N$ such that $b(n, n') = b(x, n')$ for every $n \in N$. But by definition of $N^\perp$, $x - n \in N^\perp$, which implies that $x = n + (x - n)$ is the decomposition we required. □

Lemma 2.42. *Let (M, b) be an orthogonal space. Let $x_1, ..., x_n \in M$ be such that the matrix $(b(x_i, x_j))$ is invertible. Let N be the submodule of M spanned by the x_i. Then $\{x_1, ..., x_n\}$ is a linearly independent set, and $M \simeq N \oplus N^\perp$.*

Proof. Suppose for the sake of contradiction that $\{x_1, ..., x_n\}$ is not a linearly independent set. Then there exist $c_i \in R$ for $1 \leq i \leq n$, not all zero, such that $c_1x_1 + ... + c_nx_n = 0$. By bilinearity of b, for any fixed j we have $c_1b(x_1, x_j) + ... + c_nb(x_n, x_j) = 0$, contradicting invertibility of $(b(x_i, x_j))$. Therefore, $\{x_1, ..., x_n\}$ must be linearly independent. Since $(b(x_i, x_j))$ is invertible, by Lemma 2.32, b is an inner product when restricted to N. The result follows by Lemma 2.41. □

Corollary 2.43. *Let (M, b) be an orthogonal space, where M is a module over a unital commutative ring R. Then for some $n \leq \text{rank}_R(M)$,*

$$M \simeq \langle u_1 \rangle \oplus ... \oplus \langle u_n \rangle \oplus N$$

where $u_1, ..., u_n$ are units, and for every $x \in N$, $b(x, x)$ is not a unit.

Proof. If $b(y, y)$ is a unit for some $y \in M$, then by Lemma 2.42, $M \simeq Ry \oplus (Ry)^\perp$. Note that if we let $u_1 = b(y, y)$, then $Ry \simeq \langle u_1 \rangle$. Inductively, we apply the process to $(Ry)^\perp$, and for rank reasons it terminates after finitely many steps. □

Definition 2.44. Let $X = (M, b)$ be a non-degenerate orthogonal space over a unital commutative ring R. Given an R-basis $\{e_1, ..., e_n\}$ for X, we define the *dual basis* $\{e_1^*, ..., e_n^*\}$ by the conditions $b(e_i, e_k^*) = 0$ for $i \neq k$ and $b(e_i, e_i^*) = 1$ for all $1 \leq i \leq n$.

Lemma 2.45. *Let $X = (M, b)$ be a non-degenerate orthogonal space. Given a basis $\{e_1, ..., e_n\}$ for X, there exists a unique dual basis $\{e_1^*, ..., e_n^*\}$ in X.*

Proof. Under these conditions, the matrix $(b(e_i, e_j))_{1 \leq i,j \leq n}$ is invertible. Let its inverse be $(a_{k\ell})$. Consider the products $P = b(e_i, e_j)(a_{k\ell})$ and $Q = (a_{k\ell})b(e_i, e_j)$, which are equal to the identity. Then

$$[P]_{ij} = a_{1j}b(e_i, e_1) + ... + a_{nj}b(e_i, e_n), \text{ and}$$

$$[Q]_{ij} = a_{i1}b(e_1, e_j) + ... + a_{in}b(e_n, e_j).$$

Therefore, if, for $1 \leq k \leq n$, we set

$$e_k^* = a_{1k}e_1 + ... + a_{nk}e_n,$$

then $b(e_i, e_k^*) = 0$ for $i \neq k$ and $b(e_i, e_i^*) = 1$, as desired. Moreover, this is the only linear combination of $\{e_1, ..., e_n\}$ satisfying the conditions required of e_k^*. □

Remark 2.46. We sketch two alternative proofs of the previous lemma.

Alternative proof 1. Consider the 1-dimensional subspace $\text{span}\{e_2, ..., e_n\}^\perp$. Suppose it is spanned by v_1 with $b(e_1, v_1) \neq 0 \in R^\times$. Then scale v_1 so that $b(e_1, v_1) = 1$. Let $e_1^* = v_1$. Repeat this procedure for $\text{span}\{e_3, ..., e_n\}^\perp$, $\text{span}\{e_4, ..., e_n\}^\perp$, etc., to obtain e_2^*, e_3^*, and the rest in succession. □

Alternative proof 2. Define $f_i : X \to R$ by

$$e_j \mapsto \begin{cases} 0 & \text{if } j \neq i \\ 1 & \text{if } j = i \end{cases}$$

Then there exists e_i^* such that $f_i(e_j) = b(e_i^*, e_j)$ for every j. □

Definition 2.47. Let (M, b) be an orthogonal space over a unital commutative ring R. Let $M \simeq \langle u_1 \rangle \oplus ... \langle u_k \rangle \oplus N$ be a decomposition obtained by Corollary 2.43. A *unital basis* for (M, b) *with respect to that decomposition* is an R-basis $\{e_1, ..., e_n\}$ ($n = \dim_R(M)$) of M as an R-module such that $b(e_i, e_i) = u_i$ for every $1 \leq i \leq k$. A *unital basis* for (M, b) is a basis that is unital with respect to some such decomposition.

Corollary 2.48. *Let R be a unital commutative local ring in which 2 is a unit. Let (M, b) be a non-degenerate orthogonal space over R. Then (M, b) has a unital basis.*

Proof. Let $M \simeq \langle u_1 \rangle \oplus ... \oplus \langle u_n \rangle \oplus N$ be the decomposition of M obtained by Corollary 2.43. Since the restriction of b to $N \times N$ is an inner product, $(N, b|_N)$ is a non-degenerate orthogonal space. It suffices to prove that N is trivial. Suppose not. Since N is an orthogonal space, hence free, we can choose a basis $\{e_1, ..., e_k\}$ of N. Let $\{e_1^*, ..., e_k^*\}$ be the dual basis. By definition of the dual basis of a free module, we have $b(e_1, e_1^*) = 1$. Thus

$$2 = 2b(e_1, e_1^*) = b(e_1 + e_1^*, e_1 + e_1^*) - b(e_1, e_1) - b(e_1^*, e_1^*).$$

Since non-units form an ideal in any local ring, 2 is a non-unit, contradicting the assumption that it is a unit. It follows that N is trivial, so $X \simeq \langle u_1 \rangle \oplus ... \oplus \langle u_n \rangle$. There is an element e_i such that $b(e_i, e_i) = u_i$, and $\{e_1, ..., e_n\}$ is then a unital basis. □

Definition 2.49. Let X be an orthogonal space over a unital commutative ring R. Let $X = X_1 \oplus X_2$ be an orthogonal sum decomposition. The *reflection* of X with respect to (X_1, X_2) is the linear transformation $T : X \to X$ that acts as the identity on X_1 and sends each element of X_2 to its negative. Note that T preserves the underlying bilinear form.

Lemma 2.50. *Let R be a unital commutative local ring in which 2 is a unit. Let $X = (M, b)$ be an orthogonal space over R, and let $x, y \in X$ be such that $b(x, x) = b(y, y)$ is a unit. Then there exists a reflection T such that $T(x) = y$.*

Proof. Write $x = u+v$, where $u = (x+y)/2$ and $v = (x-y)/2$. Then $b(x, x) = b(u, u)+b(v, v)$. Since $b(x, x)$ is a unit and R is a local ring, at least one of $b(u, u)$ and $b(v, v)$ is a unit. Suppose $b(u, u)$ is a unit. Then $X \simeq Ru \oplus (Ru)^\perp$ by Lemma 2.42. Let T be the reflection with respect to $(Ru, (Ru)^\perp)$. Since $x = u + v$ with respect to this direct sum decomposition, $T(x) = u - v = y$. If $b(v, v)$ is a unit instead, we can apply a similar argument, reflecting about $((Rv)^\perp, Rv)$ to send y to x. □

We are finally ready to prove *Witt's cancellation theorem.*

Theorem 2.51. *Let X, Y, Z be symmetric non-degenerate orthogonal spaces over a unital commutative local ring R in which 2 is a unit. Let Z be symmetric. Suppose $X \oplus Y \simeq X \oplus Z$. Then $Y \simeq Z$.*

Proof. It follows from Corollary 2.48 that X is an orthogonal direct sum of non-degenerate orthogonal spaces that are free of rank 1. (This is where we use the hypothesis that the spaces are symmetric.) We therefore need only prove the theorem in the case where X is free of rank 1. Suppose $\{e_1\}$ is a basis for X. Since $X \oplus Y \simeq X \oplus Z$, we can pick some isomorphism $\iota : X \oplus Y \to X \oplus Z$ of orthogonal spaces. Let 0_X, 0_Y, and 0_Z denote the zero elements of X, Y, and Z, respectively. Consider $f(e_1 \oplus 0_Y)$ and $e_1 \oplus 0_Z$, which are both elements of $X \oplus Z$. These elements satisfy the hypothesis of Lemma 2.50. Therefore, there exists some reflection T of $X \oplus Z$ such that $T(\iota(e_1 \oplus 0_Y)) = e_1 \oplus 0_Z$. Now, $T \circ \iota : X \oplus Y \to X \oplus Z$ is an isomorphism, and $(T \circ \iota)(e_1 \oplus 0_Y) = e_1 \oplus 0_Z$. Thus $T \circ \iota$ maps the perpendicular space of $0_X \oplus Y$ isomorphically to $0_X \oplus Z$, from which it follows that $Y \simeq Z$. □

The next theorem is known as *Witt's extension theorem.* The statement and proof we give are essentially those of Theorem 7.2 in [8].

Theorem 2.52. *Suppose X_1 and X_2 are isomorphic symmetric non-degenerate orthogonal spaces over a unital commutative local ring R in which 2 is a unit, and suppose they have orthogonal direct sum decompositions $X_1 = U_1 \oplus V_1$ and $X_2 = U_2 \oplus V_2$. Suppose $f : V_1 \to V_2$ is an isomorphism. Then there is an isomorphism $F : X_1 \to X_2$ such that $F|_{V_1} = f$ and $F(U_1) = U_2$.*

Proof. Since $U_1 \oplus V_1 \simeq U_2 \oplus V_2$ and $V_1 \simeq V_2$, by Theorem 2.51, $U_1 \simeq U_2$. (The hypotheses are required by the cited theorem.) Call this isomorphism f_U. Then $F = f_U \oplus f$ satisfies the required conditions. □

The following definitions are variants of ones found in [1] and [2].

Definition 2.53. [1] Let (M, b) be a non-degenerate orthogonal space, where M is over a unital commutative ring R. Let $T : M \to M$ be an R-module homomorphism. The *adjoint map* T^* is defined by the condition

$$b(Tx, y) = b(x, T^*y)$$

for every $x, y \in M$. The uniqueness of T^* for fixed T follows from non-degeneracy of (M, b). The homomorphism T is *orthogonal* if

$$b(Tx, Ty) = b(x, y)$$

for all $x, y \in M$. This condition implies that T is invertible, $T^{-1} = T^*$, and $\det(T) = \pm 1$. The *special orthogonal group* of M is defined by

$$\mathrm{SO}(M) = \{T \in \mathrm{Hom}_R(M, M) \mid TT^* = T^*T = 1, \det(T) = 1\}.$$

Note that since $b(Tx, Ty) = b(T^*Tx, y) = b(x, y)$ for all $T \in \mathrm{SO}(M)$ and all $x, y \in M$, elements of $\mathrm{SO}(M)$ are orthogonal. If M is split, we say $\mathrm{SO}(M)$ is *split* as well.

Definition 2.54. [2] Let k be a field with $\mathrm{char}(k) \neq 0$. Let W be an orthogonal space of rank n over k. Let e be a basis vector of $\wedge^n(W)$. Let $A = \langle \cdot, \cdot \rangle$ be a symmetric bilinear form in $\mathrm{Sym}_2(W^*)$, the space of symmetric bilinear forms on W. Let $\langle \cdot, \cdot \rangle_n$ be the induced symmetric bilinear form on $\wedge^n(W)$. The *discriminant* of A is defined by

$$\mathrm{disc}(A) = (-1)^{n(n-1)/2} \langle e, e \rangle_n.$$

Note that if $\{w_1, ..., w_n\}$ is a basis of W, we can take $e = w_1 \wedge ... \wedge w_n$, in which case $\langle e, e \rangle_n = \det(\langle w_i, w_j \rangle)$, where $\langle w_i, w_j \rangle$ is evaluated with respect to A (i.e., $\langle w_i, w_j \rangle = A(w_i, w_j)$).

3 Arithmetic invariant theory over fields

3.1 First principle of AIT

Let G be a group scheme over a field k with a representation V. Let K/k be a field extension. We will occasionally refer to a $G(K)$-orbit of an element $v \in V(K)$ as a *K-orbit* for short.

The following lemma, which we dub the *first principle for AIT over fields*, is the key to classifying k-orbits lying within a given k^s-orbit and is the foundation on which AIT is built.

Lemma 3.1. *[1] Let k be a field with separable closure k^s. Let G be a group scheme over k, and let V be a representation of G on a finite-dimensional vector space over k. Suppose $v \in V(k)$ with stabilizer G_v. Then there is a bijection between the set of $G(k)$-orbits of vectors $w \in V(k)$ lying in the same $G(k^s)$-orbit as v and the kernel of the map of pointed sets*

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

in Galois cohomology.

Proof. If $w \in V(k)$ lies in the same k^s-orbit as v, then there exists $g \in G(k^s)$ such that $w = g(v)$. Note that if $h \in G_v(k^s)$, then $g(h(v)) = g(v)$, so g is only well-defined up to right multiplication by elements of $G_v(k^s)$. Let g^σ be the image of $g \in G$ under the action of $\sigma \in \mathrm{Gal}(k^s/k)$. Define

$$a_\sigma = g^{-1} g^\sigma \in G(k^s).$$

We claim the map $\sigma \mapsto a_\sigma$ is a 1-cocycle with values in $G(k^s)$. Because $G(k^s)$ is equipped with the discrete topology, to check that the map is continuous, it suffices to check that the preimage of every point is open. The preimage of a point is of the form $\tau\Gamma_g$ where $\Gamma_g = \{\sigma \in \mathrm{Gal}(k^s/k) | g^\sigma = g\}$. If Γ_g is open, the translates $\tau\Gamma_g$ will certainly be open. The stabilizer Γ_g is open by the argument from the proof of Lemma 2.17.

Also, for $g \in G(k^s)$ and $\sigma, \tau \in \mathrm{Gal}(k^s/k)$, we calculate

$$ga_{\sigma\tau} = g^{\sigma\tau} = (ga_\tau)^\sigma = ga_\sigma a_\tau^\sigma,$$

so $a_{\sigma\tau} = a_\sigma a_\tau^\sigma$, which is precisely the 1-cocycle condition.
Moreover, $a_\sigma \sim_{\mathrm{coho},1} 1$ in $H^1(k, G)$ by definition of a_σ. Since the Galois action fixes the elements of $V(k)$, we have

$$a_\sigma(v) = g^{-1}g^\sigma(v) = g^{-1}g^\sigma(v^\sigma) = g^{-1}(w^\sigma) = g^{-1}(w) = v,$$

which shows that $a_\sigma \in G_v(k^s)$, so we can in fact view $(\sigma \mapsto a_\sigma)$ as a 1-cocycle with values in $G_v(k^s)$. We note that the cohomology class of $(\sigma \mapsto a_\sigma)$ as a 1-cocycle with values in $G_v(k^s)$ does not depend on the choice of g and that $(\sigma \mapsto a_\sigma)$ is an element of $\ker(\gamma)$.

Conversely, given an element $(\sigma \mapsto a_\sigma) \in \ker(\gamma)$, the image of the class of $(\sigma \mapsto a_\sigma)$ is trivial in $H^1(k, G)$, so there exists $g \in G(k^s)$ such that

$$a_\sigma = g^{-1}g^\sigma.$$

Let $w = g(v)$. Then

$$w^\sigma = g^\sigma(v^\sigma) = g^\sigma(v) = ga_\sigma(v) = g(v) = w.$$

Therefore, $w \in V(k)$, and w lies in the same $G(k^s)$-orbit as v. □

We observe that if the map γ in Lemma 3.1 is injective, then the arithmetic invariant theory of the representation coincides with its geometric invariant theory.

3.2 Preamble to examples

Theorem 3.2. *Let G be a reductive group scheme over a field k acting on some representation V. Let k^s be a separable closure of k. Let $k[V]^G$ denote the algebra of G-invariant polynomials on V. Suppose we wish to prove that $k[V]^G$ is freely generated by some candidate generating set $\{p_1, ..., p_n\}$. It suffices to work over k^s. Let $inv : V \to \mathbb{A}^n$ be defined by*

$$inv(v) = (p_1(v), ..., p_n(v)).$$

Suppose there exists a regular map $s : \mathbb{A}^n \to V$ such that given values $r_1, ..., r_n$ of $p_1, ..., p_n$, respectively, $p_i(s(r_1, ..., r_n)) = r_i$ for all $1 \leq i \leq n$. Consider the following two statements.

(i) Each element of the set $\{p_1, ..., p_n\}$ is an invariant polynomial.

(ii) For any separably closed field extension K/k and generic points $v, w \in V(K)$ satisfying $p_i(v) = p_i(w)$ for all $1 \leq i \leq n$, there exists $g \in G(k^s)$ such that $g(v) = w$.

Under our assumptions, if (i) and (ii) hold, then $\{p_1, ..., p_n\}$ generates $k[V]^G$.

Proof. Step (i) is clearly necessary. Note that existence of the map s implies that given arbitrary values $r_1, ..., r_n$ of $p_1, ..., p_n$, respectively, there exists some $v \in V(k^s)$ such that $p_i(v) = r_i$ for all $1 \leq i \leq n$. Therefore, there are no relations among the p_i, i.e., there is no non-trivial polynomial q such that $q(p_1, ..., p_n) = 0$, since that would imply that the p_i cannot take arbitrary values, a contradiction.

It remains to prove that, under the assumption of (ii), $\{p_1, ..., p_n\}$ generates $k[V]^G$. Let $p \in k[V]^G$, and let $v \in V(k[x_1, ..., x_{\dim(V)}])$ be the generic point. We wish to show that p is a polynomial in $p_1, ..., p_n$. By our assumption about the existence of the map s, for every $1 \leq i \leq n$,

$$p_i(v) = p_i(s(\text{inv}(v))).$$

By the assumption we made at the start of step (ii), there exists $g \in G(k^s)$ such that $s(\text{inv}(v)) = g(v)$. Since p is G-invariant,

$$p(s(\text{inv}(v))) = p(g(v)) = p(v).$$

But since s is a regular map and p is a polynomial, $p(s(\text{inv}(v)))$ will be some polynomial in the p_i, which means p is in the algebra generated by the p_i, as desired. □

Let W be a non-degenerate split orthogonal space over a field k with characteristic not equal to 2. Suppose W has odd dimension $2n + 1$ where $n \geq 1$ and has determinant $(-1)^n \in k^\times/k^{\times 2}$, so that it has discriminant 1. Suppose further that W has a k-basis $\{e_1, e_2, ..., e_n, u, f_n, ..., f_2, f_1\}$ and an inner product defined by

$$\langle e_i, e_j \rangle = \langle f_i, f_j \rangle = \langle e_i, u \rangle = \langle f_i, u \rangle = 0, \langle e_i, f_j \rangle = \delta_{ij}, \langle u, u \rangle = 1.$$

Then $G = \text{SO}(W)$ is a reductive group over k. We will now consider three different representations V of G: first, the standard representation $V = W$; second, the adjoint representation $\mathfrak{so}(W) \simeq \wedge^2(W)$; and third, the symmetric square representation $\text{Sym}^2(W)$, which we now define.

Definition 3.3. Let V be a finite-dimensional representation. Let $\{e_1, ..., e_n\}$ be a basis for V. Let S be the endomorphism of $V \otimes V$ defined by $S(e_i \otimes e_j) = e_j \otimes e_i$. The *symmetric square* of V is defined by

$$\text{Sym}^2(V) = \{v \in V \otimes V \mid S(v) = v\}.$$

For each of these representations, we will determine the ring $k[V]^G$ of polynomial invariants and describe the orbits via Lemma 3.1.

3.3 Example 1: The standard representation

First, we consider the standard representation $V = W$. We assume $\mathrm{char}(k) \neq 2$. This representation is irreducible of dimension $\dim(V) = 2n + 1$.

When $V = W$, we claim the invariant $q_2(v) = \langle v, v\rangle$ generates the ring of invariant polynomials. As an example, we will show how to apply Theorem 3.2 to prove this. In later cases, we will just cite that remark. The section s from Theorem 3.2 is given by $d \mapsto e_1 + \frac{1}{2}df_1$.

(i) Observe that since $g \in \mathrm{SO}(W)$ is orthogonal, $\langle gv, gv\rangle = \langle v, v\rangle$ for all v.

(ii) If two vectors $v, w \in V(k^s)$ have the same inner product, we claim that there exists some element of the rotation group $\mathrm{SO}(W)(k^s)$ sending one to the other. When $v = w$, the identity is such an element. When v and w are distinct vectors, there are two cases. First, suppose $\langle v - w, v - w\rangle \neq 0$. Then the reflection

$$x \mapsto x - \frac{2\langle x, v - w\rangle}{\langle v - w, v - w\rangle}(v - w)$$

sends v to w, and composing it with any reflection that fixes w, we obtain an element of $\mathrm{SO}(W)(k^s)$ sending v to w.

Next, suppose $\langle v-w, v-w\rangle = 0$. This occurs precisely when $\langle v, v\rangle = \langle v, w\rangle = \langle w, w\rangle$. Choose a vector u such that $\langle u, w\rangle \neq \langle w, w\rangle$ and $\langle u, v\rangle \neq \langle v, v\rangle$. By solving a linear equation, we can find c such that $\langle u + c(v - w), u + c(v - w)\rangle = \langle v, v\rangle$, which is necessarily equal to $\langle w, w\rangle$. We have $\langle u + c(v - w), v\rangle = \langle u, v\rangle \neq \langle v, v\rangle$ and similarly $\langle u + c(v - w), w\rangle \neq \langle w, w\rangle$. We can now apply the previous case to find reflections in $\mathrm{SO}(W)(k^s)$ that send v to $u + c(v - w)$ and that send $u + c(v - w)$ to w. The composition of these two maps gives an element of $\mathrm{SO}(W)(k^s)$ that sends v to w, as desired.

Since (i) to (ii) are satisfied, $q_2(v)$ generates the ring of invariant polynomials as claimed.

We define $\Delta = q_2$ in this case. Since special orthogonal groups are rotation groups, we see geometrically that for $\Delta(v) \neq 0$, the stabilizer G_v is the reductive subgroup $\mathrm{SO}(U)$, where U is the hyperplane in W of vectors orthogonal to v.

Note that a bilinear form can be defined on the subspace U by restricting the inner product on V, and the resulting bilinear form is non-degenerate by Remark 2.38. A Gram matrix can be obtained for forms obtained by restriction from the matrix defining the original form by a combination of changing the basis and restricting to a submatrix.

We now classify orbits over k. Let $d \in k^\times$, and consider the vector $v = e_1 + \frac{1}{2}df_1$. Observe that $q_2(v) = \Delta(v) = d$, which shows that there exist vectors $v \in V(k^s)$ with arbitrary values of $q_2(v)$. We see geometrically that the stabilizer G_v acts on the perpendicular space $U' = (kv)^\perp$ in W, and indeed we can make the identification $G_v = \mathrm{SO}(U')$. By choosing an

element in $\mathrm{SO}(W)(k)$ that is an isomorphism from kv to kw and applying Witt's extension theorem to $(kv) \oplus (kv)^{\perp} = (kw) \oplus (kw)^{\perp}$, all vectors w with $q_2(w) = d$ lie in the same $G(k)$-orbit as v, and it follows that the invariant polynomials separate the orbits over k with non-zero discriminant. The vector $v = e_1$ also gives a single non-zero orbit with $q_2(v) = 0$.

We now wish to compare this work with the first principle of AIT. To calculate $H^1(k, \mathrm{SO}(U))$, we observe that by [26] it classifies non-degenerate orthogonal spaces U' of dimension $2n$ and discriminant d over k. Similarly, $H^1(k, \mathrm{SO}(W))$ classifies non-degenerate orthogonal spaces W' of dimension $2n+1$ and determinant $(-1)^n$ over k. The trivial class corresponds to W itself. The map

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

is then given by $U' \mapsto U' \oplus \langle d \rangle$. By Witt's cancellation theorem, γ is injective, which means the arithmetic invariant theory of odd orthogonal groups coincides with their geometric invariant theory in this case.

3.4 Example 2: The adjoint representation

The second representation is the adjoint representation $V = \mathfrak{so}(W)$. This representation is irreducible, and the dimension of the corresponding Lie algebra (hence the representation) is $2n^2 + n$.

The adjoint representation is isomorphic to the exterior square $\wedge^2(W)$. We can realize it as

$$V = \{T : W \to W \mid T = -T^*\}$$

with $g \in G$ acting by

$$g \cdot T = gTg^{-1} = gTg^*, T \in V.$$

The characteristic polynomial is an invariant of any $G(k)$-orbit.

Any operator $T \in V$ is skew self-adjoint, so its characteristic polynomial is of the form

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

with $c_{2m} \in k$ for all m. The coefficients c_{2m} are polynomial invariants of the representation, and these polynomials generate the ring of invariant polynomials of V over k and are algebraically independent by [7]. Let Δ be the discriminant of $f(x)$, which is also an invariant because it lies in the algebra generated by the coefficients c_{2m}. Note that $\Delta \neq 0$ if and only if $f(x)$ is separable.

Suppose

$$f(x) = x^{2n+1} + c_2 x^{2n-1} + c_4 x^{2n-3} + ... + c_{2n} x \in k[x]$$

has non-zero discriminant. We will construct a skew self-adjoint operator T on W with

characteristic polynomial $f(x)$. This construction will serve as the section s from Theorem 3.2. Writing $f(x) = xh(x) = xg(x^2)$ for appropriate $h(x)$ and $g(x)$, by the standard formula for the discriminant of products of polynomials, we have

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

Let $K = k[x]/(g(x))$, $E = k[x]/(h(x))$, and $L = k[x]/(f(x))$. Note that $L \simeq K \oplus k$. Since we assumed that $\Delta \neq 0$, these are étale k-algebras of ranks n, $2n$, and $2n+1$, respectively. The map $x \mapsto -x$ induces an involution τ of the algebras E and L. The corresponding fixed algebras are K and $K \oplus k$, respectively. Let β be the image of x in L.

Observe that L can be viewed as the k–vector space with basis $\{1, \beta, ..., \beta^{2n}\}$. We can define a symmetric bilinear form on this space by letting $\langle \lambda, \mu \rangle$ be the coefficient of β^{2n} in $(-1)^n \lambda \mu^\tau$. This form is non-degenerate with discriminant 1, and the map $t(\lambda) = \beta\lambda$ is skew self-adjoint with characteristic polynomial $f(x)$. The subspace $M = k \oplus k\beta \oplus ... \oplus k\beta^{n-1}$ is isotropic of dimension n, so L is split and isomorphic to W over k. Choosing an isometry $\theta : L \to W$ allows us to define a skew self-adjoint operator $T = \theta t \theta^{-1}$ on W with characteristic polynomial $f(x)$. The orbit of T is well-defined since θ is unique up to composition with an orthogonal transformation of W. The stabilizer subgroup G_T is a maximal torus in $G = \mathrm{SO}(W)$ of dimension n over k.

Over k^s, a separable closure of k, the classification of orbits is relatively easy.

Proposition 3.4. *[1] Let k be a field with separable closure k^s. Let $G = SO(W) = SO_{2n+1}$ be the split odd special orthogonal group over k. Let $S, T \in V(k^s)$ be skew self-adjoint operators. Suppose they both have separable characteristic polynomial $f(x)$. Then they lie in the same $G(k^s)$-orbit of $V(k^s)$.*

Proof. Since $f(x)$ is separable, it is the minimal polynomial of S and T. Therefore, there exists some $g \in \mathrm{GL}(W)$ with $S = gTg^{-1}$. Since S and T are skew self-adjoint, 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 $L^\times$ and its determinant is a square in $k^\times$, we see that g^*g is an element of $K^\times \times k^{\times 2}$. The fixed algebra of L under τ is $K \oplus k$, so any element x in this fixed algebra has norm $x^{1+\tau} = x^2$. Suppose k is separably closed. Then every element of $K^\times \times k^{\times 2}$ is a square, hence a norm. Let $h \in K^\times \times k^\times$ be such that $h^{1+\tau} = g^*g$. Then gh^{-1} is an orthogonal transformation of W over k^s that maps T to S, so S is in the same $G(k^s)$-orbit as T. □

Since the stabilizer G_T is abelian, $H^1(k, G_T)$ is an abelian group. Note that $G_T = (\mathrm{Res}_{E/k}(\mathbb{G}_m))_{1+\tau=\mathrm{id}}$, so we have a short exact sequence

$$1 \to G_T \to \mathrm{Res}_{E/k}(\mathbb{G}_m) \xrightarrow{N_{E/k}=1+\tau} \mathrm{Res}_{K/k}(\mathbb{G}_m) \to 1,$$

where $N_{E/k}$ denotes the norm map. Taking cohomology gives the exact sequence

$$E^\times \xrightarrow{N} K^\times \to H^1(k, G_T) \to 1$$

from which it follows that $H^1(k, G_T) \simeq K^\times / NE^\times$.

The map

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

is given as follows. Associate to $\kappa \in K^\times$ the element $\alpha = (\kappa, 1) \in (L^\tau)^\times = K^\times \times k^\times$, which has square norm from $L^\times$ to $k^\times$. Then associate to α the vector space L with the new bilinear form $\langle \lambda, \mu \rangle_\alpha$ defined to be equal to the coefficient of β^{2n} in $(-1)^n \alpha \lambda \mu^\tau$. Call the resulting orthogonal space W_κ. It has dimension $2n+1$ (because L does) and determinant $(-1)^n$ over k. The next result is related to this construction.

Proposition 3.5. *[26], [1] Let W be an orthogonal space over a field k, and let k^s be a separable closure of k. Then 1-cocycles $Gal(k^s/k) \to SO(W)(k^s)$ (i.e., elements of $H^1(k, SO(W))$) correspond to orthogonal spaces over k.*

Proof. If g is such a 1-cocycle, then we define an orthogonal space W_g over k corresponding to g as follows. Note that there is an inclusion $\mathrm{SO}(W) \to \mathrm{GL}(W)$, which induces an inclusion $H^1(k, \mathrm{SO}(W)) \to H^1(k, \mathrm{GL}(W))$. Also, $H^1(k, \mathrm{GL}(W))$ is trivial by Theorem 2.21. Therefore, using the aforementioned inclusion, we can write $g_\sigma = h^{-1} h^\sigma$ for some $h \in \mathrm{GL}(W)(k^s)$.

Now we are ready to define the orthogonal space W_g. Its underlying module is the same as the underlying vector space of W, and it is equipped with a k-valued non-degenerate symmetric bilinear form defined by

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

for all v, w in that vector space.

The resulting orthogonal space W_g has dimension $2n+1$ and determinant $(-1)^n$. Moreover, the isomorphism class of W_g over k is determined entirely by the cohomology class of g_σ in $H^1(k, G)$. □

Lemma 3.6. *[1] Let $G = SO(W)$. Let v be a vector, and let $\gamma : H^1(k, G_v) \to H^1(k, G)$ be the canonical map in cohomology. The class $\gamma(\kappa) \in H^1(k, G)$ is represented by the orthogonal space W_κ.*

Proof. We simply apply the construction of Proposition 3.5. In our case, the 1-cocycle g representing $\gamma(\kappa)$ comes from a 1-cocycle with values in the stabilizer G_v. This stabilizer is a maximal torus in $\mathrm{SO}(W)$ which is a subgroup of the larger maximal torus $\mathrm{Res}_{L/k}(\mathbb{G}_m)$ of $\mathrm{GL}(W)$. But $H^1(k, \mathrm{Res}_{L/k}(\mathbb{G}_m))$ is trivial, so there exists $h \in (L \otimes k^s)^\times$ with $h^{1+\tau} = \alpha$ (i.e., with norm α) and $g_\sigma = h^{-1} h^\sigma$. Substituting h into (1) completes the proof. □

3.5 Example 3: The symmetric square representation

The third representation is the symmetric square $V = \mathrm{Sym}^2(W)$. Here again G acts by conjugation. It has dimension $2n+1$, and since it contains the trivial subspace spanned by the identity matrix, it is not irreducible.

Just as when $V = \wedge^2(W)$, in the present case the group G acts by conjugation on V, so the characteristic polynomial is again an invariant of any $G(k)$-orbit.

The operators $T \in V$ are self-adjoint, so their characteristic polynomial will have the form

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

with coefficients $c_m \in k$ for all m. The c_m are degree m polynomial invariants that generate the ring of polynomial invariants of V over k and are algebraically independent. The discriminant $\Delta = \mathrm{disc}(f(x))$ is non-zero if and only if $f(x)$ is separable, just as before.

Suppose

$$f(x) = x^{2n+1} + c_1 x^{2n} + ... + c_{2n+1}$$

is separable. We wish to construct a self-adjoint operator $T \in V$ with characteristic polynomial $f(x)$. Let $L = k[x]/(f(x))$, and let β be the image of x in L. Define a non-degenerate symmetric bilinear form on the k–vector space $L = k \oplus k\beta \oplus ... \oplus k\beta^{2n}$ by

$$\langle \lambda, \mu \rangle_\alpha = \text{ the coefficient of } \beta^{2n} \text{ in } \alpha\lambda\mu.$$

This bilinear form has determinant $(-1)^n$, and the map $t(\lambda) = \beta\lambda$ is self-adjoint with characteristic polynomial $f(x)$. The subspace M spanned by $\{1, \beta, ..., \beta^{n-1}\}$ is isotropic of dimension n. Thus L is isomorphic to W over k. Picking an isometry $\theta : L \to W$ allows us to define the self-adjoint operator $T = \theta t \theta^{-1}$ on W with characteristic polynomial $f(x)$, as desired. Observe that θ is unique up to composition with an orthogonal transformation of W, so the orbit of T is well-defined. The stabilizer subgroup G_T is the kernel of the norm map $\mathrm{Res}_{L/K}(\mu_2) \to \mu_2$, which is a finite étale group scheme of order 2^{2n}.

Proposition 3.7. *[1] Let k be a field with separable closure k^s. Let $G = SO(W) = SO_{2n+1}$ be the odd special orthogonal group over k. Let $S, T \in V(k^s)$ be self-adjoint operators. Suppose they both have separable characteristic polynomial $f(x)$. Then they lie in the same $G(k^s)$-orbit.*

Proof. Since $f(x)$ is separable, it is the minimal polynomial of S and T. Therefore, there exists some $g \in \mathrm{GL}(W)$ with $S = gTg^{-1}$. Since S and T are self-adjoint, g^*g is in the centralizer of T in $\mathrm{GL}(W)$. The centralizer of T in $\mathrm{End}(W)$ is the algebra $k[T] = L$. Thus $g^*g \in L^\times$. But over a separable closure, every element of $L^\times$ is a square, so $g^*g = h^2$ for some $h \in L^\times$. Then gh^{-1} is an orthogonal transformation of W over k^s mapping T to S, so S lies in the same $G(k^s)$-orbit as T. □

Now that we have characterized the $G(k^s)$-orbits, we may use the first principle of AIT to characterize the $G(k)$-orbits. Over k, the stabilizer G_T is abelian, so $H^1(k, G_T)$ is an abelian group. Indeed, $G_T = (\mathrm{Res}_{L/k}(\mu_2))_{N=1}$, so we have a short exact sequence

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

Taking cohomology, we see that $H^1(k, G_T) \simeq (L^\times/L^{\times 2})_{N=1}$. The map

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

may be defined as follows. Given $\alpha \in (L^\times)_{N=1}$, consider the orthogonal space L defined by the bilinear form

$$\langle \lambda, \mu \rangle_\alpha = \text{ the coefficient of } \beta^{2n} \text{ in } \alpha\lambda\mu.$$

The orthogonal space W_α defined by this bilinear form has dimension $2n+1$ and determinant $(-1)^n$ over k. Moreover, it is determined up to isomorphism by the image of α in $H^1(k, G_T) = (L^\times/L^{\times 2})_{N=1}$. The proof that W_α represents the class $\gamma(\alpha) \in H^1(k, G)$, is the same as the proof of Lemma 3.6.

4 Obstructions to lifting k-rational orbits over fields

4.1 Pure inner forms

Definition 4.1. [26] Let G be a reductive algebraic group acting on a representation V over k. Polynomials on V can be identified with the space $k[V]^G$. We thus define a space, called the *GIT quotient*, by

$$V /\!\!/ G = \mathrm{Spec}(k[V]^G).$$

Since this is a categorical quotient, there is a canonical morphism $\pi : V \to V /\!\!/ G$. (See [24] for the relevant details about GIT and categorical quotients.) The fibres of this morphism can be identified with certain G-orbits on V. Sometimes we are lucky and can produce a canonical section of the morphism π, i.e., a canonical map $s : V /\!\!/ G \to V$ such that $\pi \circ s$ is the identity, in which case all k-rational points of $V /\!\!/ G$ lift to k-rational points of V. However, such a section does not always exist.

One notable case where such a section may not exist is the action of odd orthogonal groups $\mathrm{SO}(W')$ that are *not* split over k. The odd orthogonal groups we have considered up until now have all been split. We will now describe some non-split groups by introducing more notions from Galois cohomology.

Definition 4.2. Let G be an algebraic group with a representation V over the field k. Let $\sigma \mapsto c_\sigma$ be a 1-cocycle from $\mathrm{Gal}(k^s/k)$ to $G(k^s)$, where k^s denotes a separable closure of k. Then $c_{\sigma\tau} = c_\sigma c_\tau^\sigma$ for all $\sigma, \tau \in \mathrm{Gal}(k^s/k)$. The *pure inner form* G^c of G over k is described by giving its k^s-points and a Galois action. Let $G^c(k^s) = G(k^s)$, and let the Galois action be given by

$$\sigma(h) = c_\sigma h^\sigma c_\sigma^{-1}.$$

Note that if $g \in G(k^s)$ and $b_\sigma = g^{-1} c_\sigma g^\sigma$ is a 1-cocycle that is cohomologous to c, then the map on k^s-points $G^b \to G^c$ given by $h \mapsto ghg^{-1}$ commutes with the Galois actions, so it gives an isomorphism over k. It follows that up to isomorphism, G^c is determined over k by the image of c in $H^1(k, G)$.

Given a 1-cocycle $c : \mathrm{Gal}(k^s/k) \to G(k^s)$ and a homomorphism $\rho : G \to \mathrm{GL}(V)$, we can form a 1-cocycle $\rho(c) : \mathrm{Gal}(k^s/k) \to \mathrm{GL}(V)(k^s)$. By Theorem 2.21,

$$H^1(k, \mathrm{GL}(V)) = 1.$$

Thus there exists some $g \in \mathrm{GL}(V)(k^s)$, well-defined up to left multiplication by $\mathrm{GL}(V)(k)$, such that

$$\rho(c_\sigma) = g^{-1} g^\sigma$$

for every $\sigma \in \mathrm{Gal}(k^s/k)$. We can use this g to define a twisted representation of G^c on V over k. Indeed, the homomorphism $\rho_g : G^c(k^s) \to \mathrm{GL}(V)(k^s)$ given by

$$\rho_g(h) = g\rho(h)g^{-1}$$

commutes with the Galois actions and therefore gives a representation over k. Note that if $G(k^s)$ acts on a subset $T \subseteq V(k^s)$, then this definition by conjugation means that $G^c(k^s)$ acts on $gT \subseteq V^c(k^s)$

Since g is well-defined up to left multiplication by an element $a \in \mathrm{GL}(V)(k)$, it is important to know whether ρ_g is in fact determined up to isomorphism independently of the $\mathrm{GL}(V)(k)$-multiple of g. Indeed, if $g' = ag$, then conjugation by a gives an isomorphism from ρ_g to a representation ρ'_g. The isomorphism class of this representation depends only on c, so we may justifiably write V^c for it.

Next, let f be a rational point of $V /\!\!/ G$, and let V_f be the corresponding fibre in V induced by the canonical morphism $\pi : V \to V /\!\!/ G$. Assume that $V_f(k) \neq \emptyset$ and that $G(k^s)$ acts transitively on $V_f(k^s)$. Let $v \in V_f(k)$, and let G_v be the stabilizer of v in G.

Note that $G(k)$ acts on $V_f(k)$. We know from the first principle of AIT that $G(k)$-orbits on $V_f(k)$ are in bijection with elements of

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

this being the canonical map γ induced by the inclusion $G_v \to G$. We now generalize this to a parameterization of orbits of twists $G^c(k)$ with $c \in H^1(k, G)$. By hypothesis, $G^c(k^s) = G(k^s)$ acts transitively on $gV_f(k^s)$ in $V(k^s)$, where $g \in \mathrm{GL}(V)(k^s)$ is such that $\rho(c_\sigma) = g^{-1}g^\sigma$ for every $\sigma \in \mathrm{Gal}(k^s/k)$.

Now, we define

$$V_f^c(k) = V(k) \cap gV_f(k^s)$$

which is acted on by $G^c(k)$. The following example illuminates this abstract construction.

Example 4.3. [2] Let k be a field with $\mathrm{char}(k) \neq 2$. Let G be the group scheme μ_2 over k. Let V be the non-trivial one-dimensional representation of G on k, which is equivalent to just the standard representation of the orthogonal group $O(1)$ over k. By Theorem 3.2, its polynomial invariants are generated by $q(x) = x^2$, so the geometric quotient $V /\!\!/ G$ is the

affine line. Let f be a non-zero rational invariant in k. The fibre V_f is then the subscheme of V defined by $\{x \mid x^2 = f\}$. Thus $V_f(k) \neq \emptyset$ if and only if f is a square in $k^\times$. This holds over k^s, and $G(k^s)$ acts simply transitively on $V_f(k^s)$.

Note that $H^1(k, G) = k^\times / k^{\times 2}$ by Corollary 2.24. Any $c \in k^\times$ defines a 1-cocycle $c_\sigma = \sqrt{c}^\sigma / \sqrt{c}$ that is $G(k^s)$-valued and whose class in $H^1(k, G)$ only depends on the image of c modulo elements of $k^{\times 2}$. Then $g = \sqrt{c} \in \mathrm{GL}(V)(k^s)$ trivializes this class in $H^1(k, \mathrm{GL}(V))$. The pure inner form G^c and corresponding representation V^c remain the same, but

$$V_f^c(k) = V(k) \cap gV_f(k^s) = \{x \in k^\times \mid x^2 = fc\}.$$

Therefore, $V_f^c(k) \neq \emptyset$ if and only if $fc \in k^{\times 2}$. Moreover, given any f, there is a unique pure inner form G^c for which V_f^c has k-rational points, in which case $G^c(k)$ acts simply transitively on $V_f^c(k)$.

We are now ready to generalize the first principle of AIT.

Proposition 4.4. *[2] Let G be an algebraic group with representation V. Suppose there exists $v \in V(k)$ with invariant $f \in (V /\!\!/ G)(k)$ and stabilizer G_v such that the action of $G(k^s)$ on $V_f(k^s)$ is transitive. Then for every 1-cocycle c, there is a bijection between the set of $G^c(k)$-orbits on $V_f^c(k)$ and the elements of the fibre $\gamma^{-1}(c)$ of*

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

above $c \in H^1(k, G)$. In particular, the set of pure inner forms of G for which f lifts to a k-rational orbit of G^c on V^c is determined by the image $\gamma(H^1(k, G_v))$ in $H^1(k, G)$, and for $c = 1$ we recover the first principle of AIT.

Proof. Let c be a $G(k^s)$-valued 1-cocycle. Let $g \in \mathrm{GL}(V)(k^s)$ be such that $c_\sigma = g^{-1} g^\sigma$ for all $\sigma \in \mathrm{Gal}(k^s/k)$.

Suppose $V_f^c(k) \neq \emptyset$. We wish to show that $c \in \gamma(H^1(k, G_v))$. Let $w \in V_f(k^s)$ for which $gw \in V_f^c(k)$. Since we assumed that $G(k^s)$ acts transitively on $V_f(k^s)$, we can find $h \in G(k^s)$ such that $w = hv$. By our assumption that $gw \in V_f^c(k)$, for every $\sigma \in \mathrm{Gal}(k^s/k)$ we have $c_\sigma h^\sigma v = hv$, so

$$h^{-1} c_\sigma h^\sigma \in G_v.$$

Hence, $(\sigma \mapsto c_\sigma) \sim_{\mathrm{coho},1} (\sigma \mapsto h^{-1} c_\sigma h^\sigma)$, which belongs to $\gamma(H^1(k, G_v))$.

Now suppose that $c \in \gamma(H^1(k, G_v))$. We show that $V_f^c(k) \neq \emptyset$. Assume without loss of generality that $c_\sigma \in G_v(k^s)$ for every $\sigma \in \mathrm{Gal}(k^s/k)$. Set $w = gv \in V_f^c(k^s)$. Then if $\sigma \in \mathrm{Gal}(k^s/k)$, we have

$$w^\sigma = g c_\sigma v = gv = w.$$

It follows that $w \in V_f^c(k)$, so there is a bijection between $G^c(k) \setminus V_f^c(k)$ and $\ker(\gamma_c)$ where γ_c is the canonical map

$$\gamma_c : H^1(k, G_w^c) \to H^1(k, G^c).$$

It remains to prove that there is a bijection between $\gamma^{-1}(c)$ and $\ker(\gamma_c)$. We claim there are maps $\gamma^{-1}(c) \to \ker(\gamma_c)$ given by

$$(\sigma \mapsto d_\sigma) \mapsto (\sigma \mapsto d_\sigma c_\sigma^{-1})$$

and $\ker(\gamma_c) \to \gamma^{-1}(c)$ given by

$$(\sigma \mapsto a_\sigma) \mapsto (\sigma \mapsto a_\sigma c_\sigma).$$

We must verify that these maps are well-defined. Suppose $(\sigma \mapsto d_\sigma) \in \gamma^{-1}(c)$. We need to prove that $(\sigma \mapsto d_\sigma c_\sigma^{-1})$ is a 1-cocycle in $\ker(\gamma_c)$. Observe that for all $\sigma, \tau \in \mathrm{Gal}(k^s/k)$, we have

$$(d_\sigma c_\sigma^{-1}) \cdot \sigma(d_\tau c_\tau^{-1}) \cdot (d_{\sigma\tau} c_{\sigma\tau}^{-1})^{-1} = d_\sigma c_\sigma^{-1} (c_\sigma d_\tau^\sigma (c_\tau^{-1})^\sigma c_\sigma^{-1})(d_{\sigma\tau} c_{\sigma\tau}^{-1})^{-1} = 1.$$

Also, we can find $h \in G(k^s)$ such that for every $\sigma \in \mathrm{Gal}(k^s/k)$ we have

$$d_\sigma = h^{-1} c_\sigma h^\sigma$$

and therefore have

$$h^{-1}\sigma(h) = h^{-1} c_\sigma h^\sigma c_\sigma^{-1} = d_\sigma c_\sigma^{-1}.$$

It follows that $(\sigma \mapsto d_\sigma c_\sigma^{-1}) \in \ker(\gamma_c)$. Likewise, we can show that the second map is well-defined. Since these two maps are inverses, we have proved the claim. □

Let $f \in (V /\!\!/ G)(k)$ be an invariant. Suppose $G(k^s)$ acts transitively on $V_f(k^s)$. We now consider how to determine when $V_f^c(k) \neq \emptyset$ for a given $c \in H^1(k, G)$. In other words, we consider the problem of determining when a rational invariant lifts to a rational orbit for some pure inner form of G. A general principle in mathematics suggests that if solutions are given by H^1, then obstructions to their existence are given by the vanishing of a class in H^2. Under the assumption that G_v is abelian for every $v \in V_f(k^s)$, we show that the stabilizers G_v are canonically isomorphic to some commutative k-group scheme G_f depending only on f. Then we construct a class $d_f \in H^2(k, G_f)$ such that if $d_f \neq 0$, the orbit does not descend to k, and such that if $d_f = 0$, there exists a pure inner form of G that has k-orbits with invariant f.

The following method for obtaining the group scheme G_f is from [2]. We suppose that G is an algebraic group so that it is of finite type over k. Then the canonical map $G \times V_f \to V_f$ will be *fpqc*, i.e., faithfully flat and quasi-compact. We recall the basic definitions of *fpqc descent*.

Definition 4.5. [30, §54.15] Let S be a scheme, and let $\{f_i : S_i \to S\}_{i \in I}$ be a family of morphisms to S. We say the family is an *fpqc* (or *faithfully flat and quasi-compact*) *cover* of S if the following two conditions hold.

(i) Each f_i is flat, and the images $f_i(S_i)$ cover S.

(ii) For every affine open U of S, there exists a finite set K, a map $i : K \to I$, and affine opens $U_{i(k)} \subseteq S_{i(k)}$ such that $U = \bigcup_{k \in K} f_{i(k)}(U_{i(k)})$.

Definition 4.6. [36] Suppose $\mathcal{U} = \{U_i \to S\}_{i\in I}$ is an fpqc cover of a scheme S. Let $U_{ij} = U_i \times_S U_j$ and $U_{ijk} = U_i \times_S U_j \times_S U_k$. A *descent datum* relative to $\mathcal{U}$ is a quasi-coherent sheaf $\mathcal{F}_i$ on U_i for every $i \in I$ and an isomorphism $\varphi_{ij} : F_i|_{U_{ij}} \to F_j|_{U_{ij}}$ for all $i, j \in I$ such that $\varphi_{ik}|_{U_{ijk}} = \varphi_{jk}|_{U_{ijk}} \circ \varphi_{ij}|_{U_{ijk}}$ (the *cocycle condition*) holds for all $i, j, k \in I$. We say the descent datum *descends* or *is effective* if there exists a quasi-coherent sheaf $\mathcal{F}$ on S and a family of isomorphisms $\iota_i : \mathcal{F}|_{U_i} \to \mathcal{F}_i$ satisfying $\varphi_{ij} \circ \iota_i|_{U_{ij}} = \iota_j|_{U_{ij}}$.

According to the general theory of fpqc descent, given an fpqc map $G \times V_f \to V_f \times V_f$ as above, any descent datum will be effective. A general reference for this theory is §34 of [30]. In particular, the type of descent we apply in the following argument is *Galois descent*, a special case of fpqc descent. The relationship between Galois descent and fpqc descent is described in §34.6 of [30].

Given $v \in V_f(k^s)$ and $\sigma \in \mathrm{Gal}(k^s/k)$, we have $v^\sigma \; in V_f(k^s)$ as well, so we can choose $g_\sigma \in G(k^s)$ such that $g_\sigma v^\sigma = v$, and this g_σ is well-defined up to *left* multiplication by elements of G_v. We have isomorphisms $\theta_\sigma : (G_v)^\sigma \to G_v$ given by $h \mapsto g_\sigma h g_\sigma^{-1}$, and these are independent of the choice of g_σ because each G_v is abelian. (Indeed, the isomorphisms are trivial.) They satisfy the 1-cocycle condition $\theta_{\sigma\tau} = \theta_\sigma \circ \theta_\tau^\sigma$ for all $\sigma, \tau \in \mathrm{Gal}(k^s/k)$, so they give descent data for G_v. This descent data determines the commutative k–group scheme G_f.

Let $\iota_v : G_f(k^s) \xrightarrow{\to} \sim G_v$ be the family of canonical isomorphisms. Then if $h \in G(k^s)$ and $v \in V_f(k^s)$, we have, for every $b \in G_f(k^s)$,

$$\iota_{hv}(b) = h\iota_v(b)h^{-1}. \tag{2}$$

Moreover, for every $\sigma \in \mathrm{Gal}(k^s/k)$, $v \in V_f(k^s)$, and $b \in G_f(k^s)$, we have

$$(\iota_v(b))^\sigma = \iota_{v^\sigma}(b^\sigma). \tag{3}$$

We now construct a class $d_f \in H^2(k, G_f)$ whose triviality is equivalent to existence of a rational orbit. Let v and g_σ be as above with $g_\sigma v^\sigma = v$. Let

$$d_{\sigma,\tau} = \iota_v^{-1}(g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1}).$$

By standard arguments, $d_{\sigma,\tau}$ is a 2-cocycle whose image $d_f \in H^2(k, G_f)$ does not depend on the choice of g_σ. We also claim that $d_{\sigma,\tau}$ does not depend on the choice of $v \in V_f(k^s)$. Indeed, suppose $v' = hv \in V_f(k^s)$ where $h \in G(k^s)$. Then for any $\sigma \in \mathrm{Gal}(k^s/k)$, we have

$$hg_\sigma(h^{-1})^\sigma(v')^\sigma = hg_\sigma v^\sigma = hv = v'.$$

Furthermore, for all $\sigma, \tau \in \mathrm{Gal}(k^s/k)$, we have

$$hg_\sigma(h^{-1})^\sigma(hg\tau(h^{-1})^\tau)^\sigma(hg_{\sigma\tau}(h^{-1})^{\sigma\tau})^{-1} = hg_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1}h^{-1}.$$

Thus by (2), we find that

$$\iota_{v'}^{-1}(hg_\sigma(h^{-1})^\sigma(hg_\tau(h^{-1})^\tau)^\sigma(hg_{\sigma\tau}(h^{-1})^{\sigma\tau})^{-1}) = \iota_v^{-1}(g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1}).$$

If $V_f(k) \neq \emptyset$, then we can take v to be in $V_f(k)$, $g_\sigma = 1$, and $d_f = 0$. We summarize the above in the following result.

Proposition 4.7. *[2] Let G be a reductive algebraic group acting on a representation V over k. Suppose $f \in (V /\!\!/ G)(k)$, and suppose $G(k^a)$ acts transitively on $V_f(k^a)$ so that for every $v \in V_f(k^a)$, the stabilizer G_v is abelian. Suppose that the canonical map $G \times V_f \to V_f \times V_f$ is fppf. Let $d_f \in H^2(k, G_f)$ be constructed as above. If $V_f(k) \neq \emptyset$, then $d_f = 0$.*

A partial converse also holds. We will prove this, but first we must prove a technical lemma.

Lemma 4.8. *[2] Let G be a reductive algebraic group acting on a representation V over k. Let k^s be a separable closure of k. Let $v \in V_f(k^s)$, and let G_v be its stabilizer. Suppose $f \in (V /\!\!/ G)(k)$, and suppose $G(k^s)$ acts transitively on $V_f(k^s)$ so that for every $v \in V_f(k^s)$, the stabilizer G_v is abelian. Let g_σ be chosen as earlier so that $g_\sigma v^\sigma = v$. Then there exists a 1-cochain e_σ with values in $G_v(k^s)$ such that $(\sigma \mapsto e_\sigma g_\sigma)$ is a 1-cocycle.*

Proof. Let $\iota_v : G_f(k^s) \xrightarrow{\sim} G_v$ be a family of canonical isomorphisms. Let $\sigma \in \mathrm{Gal}(k^s/k)$. Let $b_\sigma = g^{-1} c_\sigma g^\sigma$ as earlier, and define

$$e_\sigma = \iota_v(b_\sigma^{-1}).$$

There exists g_σ such that $g_\sigma v^\sigma = v$. Then by (2) and (3), for every $\sigma \in \mathrm{Gal}(k^s/k)$ and $b \in G_f(k^s)$ we have

$$g_\sigma(\iota_v(b))^\sigma g_\sigma^{-1} = \iota_v(b^\sigma).$$

Therefore, for any $\sigma, \tau \in \mathrm{Gal}(k^s/k)$, we have

$$\begin{aligned}(e_\sigma g_\sigma)(e_\tau g_\tau)^\sigma (e_{\sigma\tau} g_{\sigma\tau})^{-1} &= \iota_v(b_\sigma^{-1}) g_\sigma(\iota_v(b_\tau^{-1}))^\sigma g_\tau^\sigma g_{\sigma\tau}^{-1} \iota_v(b_{\sigma\tau}) \\ &= \iota_v(b_\sigma^{-1}) \iota_v(b_\tau^{-1})^\sigma g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1} \iota_v(b_{\sigma\tau}) \\ &= \iota_v(b_\sigma^{-1}) \iota_v((b_\tau^{-1})^\sigma) \iota_v(b_\sigma b_\tau^\sigma b_{\sigma\tau}^{-1}) \iota_v(b_{\sigma\tau}) \\ &= 1,\end{aligned}$$

where the last equality holds because $G_f(k^s)$ is abelian by assumption. □

Theorem 4.9. *[2] Let G be a reductive algebraic group acting on a representation V over k. Suppose $f \in (V /\!\!/ G)(k)$, and suppose $G(k^s)$ acts transitively on $V_f(k^s)$ so that for every $v \in V_f(k^s)$, the stabilizer G_v is abelian. Then $d_f = 0 \in H^2(k, G_f)$ if and only if there exists a pure inner form G^c of G such that $V_f^c(k) \neq \emptyset$. In other words, $d_f = 0$ is a necessary and sufficient condition for the existence of rational orbits for some pure inner form of G.*

In particular, if $H^1(k, G) = 1$, then $G(k)$-orbits on $V_f(k)$ exist if and only if $d_f = 0$.

Proof. We claim that d_f does not depend on the pure inner form of G. Suppose $c \in H^1(k, G)$ and $g \in \mathrm{GL}(V)(k^s)$ are such that $c_\sigma = g^{-1} g^\sigma$ for every $\sigma \in \mathrm{Gal}(k^s/k)$. Take any $v \in V_f(k^s)$. Let g_σ be chosen so that $g_\sigma v^\sigma = v$ as earlier. Observe that $gv \in V_f^c(k^s)$ and

$$(g g_\sigma c_\sigma^{-1} g^{-1}) \cdot (gv)^\sigma = gv.$$

We then calculate

$$(g_\sigma c_\sigma^{-1}) \cdot \sigma(g_\tau c_\tau^{-1}) \cdot (c_{\sigma\tau} g_{\sigma\tau}^{-1}) = g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1}.$$

By that computation and Proposition 4.7, necessity holds, so we need only prove sufficiency. Note that by definition of the Galois action on a pure inner form, we have $G_v^c = G_{g^{-1}v}$ since if $g\rho(h)g^{-1}v = v$, then $\rho(h) \in G_{g^{-1}v}$. We wish to show that the collection $\{G_v^c\}$ descends to G_f just as $\{G_v\}$ does. We consider the collection of isomorphisms $\iota_v^c = \iota_{g^{-1}v} : G_f(k^s) \to G_v^c(k^s)$. Since this collection satisfies (2) and (3), we indeed obtain the same group scheme G_f in this way and thus the same class d_f.

Let $v \in V_f(k^s)$. Pick g_σ such that $g_\sigma v^\sigma = v$ for every $\sigma \in \mathrm{Gal}(k^s/k)$. If $d_f = 0$, we claim we can pick g_σ so that $(\sigma \mapsto g_\sigma)$ is a 1-cocycle and such that k-orbits exist for the pure inner twist associated to this 1-cocycle. Indeed, suppose $d_f = 0$. Let $\iota_v : G_f(k^s) \xrightarrow{\sim} G_v$ be a family of canonical isomorphisms. Then we can find a 1-cochain $(\sigma \mapsto b_\sigma)$ with values in $G_f(k^s)$ such that for every $\sigma, \tau \in \mathrm{Gal}(k^s/k)$ we have

$$g_\sigma g_\tau^\sigma g_{\sigma\tau}^{-1} = \iota_v(b_\sigma b_\tau^\sigma b_{\sigma\tau}^{-1}).$$

We now see how Lemma 4.8 completes the proof. Consider the twist of V obtained from the 1-cocycle

$$c = (\sigma \mapsto e_\sigma g_\sigma) \in H^1(k, G).$$

Choose $g \in \mathrm{GL}(V)(k^s)$ such that $g^{-1}g^\sigma = e_\sigma g_\sigma$ for every $\sigma \in \mathrm{Gal}(k^s/k)$. Then we have that $gv \in V_f^c(k)$ since, for every $\sigma \in \mathrm{Gal}(k^s/k)$,

$$(gv)^\sigma = g e_\sigma g_\sigma v^\sigma = g e_\sigma v = gv.$$

This completes the proof. □

Under a stronger assumption on the action of $G(k^s)$ on $V_f(k^s)$, it now follow that a unique pure inner form G^c renders $V_f^c(k)$ non-empty.

Corollary 4.10. *[2] Let G be a reductive algebraic group acting on a representation V over k. Suppose $f \in (V /\!\!/ G)(k)$, and suppose $G(k^s)$ acts simply transitively on $V_f(k^s)$. Then there exists a unique pure inner form G^c of G over k such that $V_f^c(k)$ is non-empty. Moreover, $G^c(k)$ acts simply transitively on $V_f^c(k)$.*

Proof. Since the action is simply transitive, therefore free, we have $G_f = 1$ in this case. It follows that $H^2(k, G_f) = 0$, so the cohomological obstruction d_f vanishes. It follows that there exists a pure inner form G^c for which rational orbits exist. Let $v_0 \in V_f^c(k)$ be a rational lift. Then since $G_{v_0} = 1$, we find that $\gamma(H^1(k, G_{v_0}^c))$ is a singleton. Therefore, no other pure inner form has a rational orbit with invariant f, and there is just one orbit of $G^c(k)$ on $V_f^c(k)$. □

4.2 Example of obstruction to lifting rational points

Let $G = \mathrm{SL}_n$. Let k be a field with $\mathrm{char}(k) \neq 2$. Let W be an n-dimensional k-vector space. Let e be a basis vector of $\wedge^n(W)$. Note that G acts on the space $\mathrm{Sym}_2(W^*)$ of symmetric

bilinear forms $\langle v, w\rangle$ on W by

$$g \cdot \langle v, v'\rangle = \langle gv, gv'\rangle$$

for all $v, v' \in W$.

By Theorem 3.2, the ring of G-invariant polynomials for this representation is generated by the discriminant, which is a polynomial of degree n.

Next, consider the action of G on $V = \mathrm{Sym}_2(W^*) \oplus \mathrm{Sym}_2(W^*)$. Let $A = \langle \cdot, \cdot \rangle_A$ and $B = \langle \cdot, \cdot \rangle_B$ be symmetric bilinear forms on W. We associate a corresponding degree n binary form over k to these symmetric bilinear forms by defining

$$f(x, y) = \mathrm{disc}(xA - yB) = f_0 x^n + f_1 x^{n-1} y + ... + f_n y^n.$$

The coefficients of $f(x, y)$ are polynomial invariants of degree n on V, and these $n + 1$ coefficients freely generate the ring of polynomial invariants for G for this representation, as we will see shortly. We call $f(x, y)$ the *invariant binary form* associated to the vector $v = (A, B)$, or more precisely, to its orbit.

Definition 4.11. Let k be a field. Let $f(x, y)$ be a degree n binary form, say

$$f(x, y) = f_0 x^n + f_1 x^{n-1} y + ... + f_n y^n.$$

Let k^a be an algebraic closure of k. Over k^a, we can factor $f(x, y)$ as

$$f(x, y) = \prod(\alpha_i x - \beta_i y)$$

for some $\alpha_i, \beta_i \in k^a$. The *discriminant* of f is defined to be

$$\Delta(f) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

Then $\Delta(f)$ is a homogeneous polynomial of degree $2n - 2$ in the f_j.

It follows from this definition that the discriminant $\Delta(f)$ is a polynomial invariant of degree $2n(n - 1)$ on V.

Theorem 4.12. *[2] Let k be a field with separable closure k^s. Let*

$$f(x, y) = f_0 x^n + f_1 x^{n-1} y + ... + f_n y^n$$

be a binary form of degree n over k^s with $f_0 \neq 0$ and $\Delta(f) \neq 0$. Let $G = SL_n$, let W be an n-dimensional k-vector space, and let $V = Sym_2(W^*) \oplus Sym_2(W^*)$. Then there exist vectors (A, B) in $V(k^s)$ whose invariant form is $f(x, y)$, and all these vectors lie in a single closed $G(k^s)$-orbit. Moreover, the stabilizer of any vector in the orbit is an elementary abelian 2-group of order 2^{n-1}.

Proof. We claim that we can find symmetric bilinear forms A and B on W over k^s such that $\mathrm{disc}(xA - yB) = f(x, y)$. Indeed, $f(x, y)$ splits into linear factors over k^s, so the claim follows from the correspondence between symmetric bilinear forms and symmetric matrices and Definition 2.54. The forms A and B both induce k^s-linear maps $W \to W^*$, which, by abuse of notation, we also denote A and B, respectively. Since $f_0 \neq 0$ by assumption, the map $A : W \to W^*$ is an isomorphism, and so is B by the same argument. Therefore, we can define an endomorphism $T = A^{-1}B : W \to W$. Since both A and B are symmetric, T is self-adjoint with respect to $\langle \cdot, \cdot \rangle_A$ on W.

Now, write $f(x, 1) = f_0 g(x)$. Observe that $\det(xI - T) = g(x)$. By assumption $\Delta(f) \neq 0$, so $g(x)$ is separable. It follows that T is regular and semisimple. Note that $G(k^s)$ acts transitively on bilinear forms with discriminant f_0, and note also that the stabilizer of A is the orthogonal group we denote by $\mathrm{SO}(W, A)$. Since $\mathrm{SO}(W, A)(k^s)$ acts transitively on self-adjoint operators T with separable characteristic polynomial equal to $g(x)$, there is only one $G(k^s)$-orbit on vectors (A, B) with invariant form $f(x, y)$. Note that the stabilizer is then the centralizer of T in $\mathrm{SO}(W, A)$, which is an elementary abelian 2-group of order 2^{n-1}. For proofs of these assertions, see Proposition 4 of [1]. □

Theorem 4.13. *[2] Let k be a field with separable closure k^s. Let*

$$f(x, y) = f_0 x^n + f_1 x^{n-1} y + ... + f_n y^n$$

be a binary form of degree n over k^s with $f_0 \neq 0$ and $\Delta(f) \neq 0$. Let $G = SL_n$, let W be an n-dimensional k-vector space, and let $V = Sym_2(W^*) \oplus Sym_2(W^*)$. Let $f(x, 1) = f_0 g(x)$. Let $L = k[x]/(g(x))$. In this setting, there is a canonical bijection between the set of orbits (A, B) of $G(k)$ on $V(k)$ with invariant binary form $f(x, y)$ and the set of equivalence classes of pairs (α, t) with $\alpha \in L^\times$ and $t \in k^\times$ satisfying

$$f_0 N(\alpha) = t^2.$$

The equivalence relation is defined by saying $(\alpha, t) \sim (\alpha', t')$ if there exists $c \in L^\times$ with $c^2\alpha' = \alpha$ and $N(c)t' = t$. Orbits having invariant $f(x, y)$ exist if and only if $f_0 \in N(L^\times)k^{\times 2}$.

Moreover, by descending the stabilizers $G_{A,B}$ for $(A, B) \in V_f(k^s)$ to k, we obtain a group scheme $G_f \simeq (Res_{L/k}(\mu_2))_{N=1}$ of order 2^{n-1} over k.

Proof. Suppose $(A, B) \in V(k)$ satisfies $\mathrm{disc}(xA - yB) = f(x, y)$. As before, A and B give two isomorphisms abusively denoted by the same variables, and we thus obtain an endomorphism $T = A^{-1}B : W \to W$ that is self-adjoint with respect to $\langle \cdot, \cdot \rangle_A$ and has $g(x)$ as its characteristic polynomial. Moreover, $g(x)$ is separable since $\Delta(f) \neq 0$ by assumption, and W is a free $L = k[T] = k[x]/(g(x))$-module of rank one. Let β be the image of x in L. Then we have a basis $\{1, \beta, \beta^2, ..., \beta^{n-1}\}$ of L over k.

Let m be a basis vector for W over L. Note that A and B arise as traces of L-bilinear forms on W. Consider the k-linear map $L \to k$ given by

$$\lambda \mapsto \langle m, \lambda m \rangle_A.$$

By separability of $g(x)$, we see that $g'(\beta) \in L^\times$. Since the trace form $(x, y) \mapsto \mathrm{Trace}(xy)$ is non-degenerate, there exists a unique $\kappa \in L^\times$ such that

$$\langle m, \lambda m \rangle_A = \mathrm{Trace}(\kappa\lambda/g'(\beta))$$

for every $\lambda \in L$. But since every element of L is self-adjoint with respect to $\langle \cdot, \cdot \rangle_A$, for every $\mu, \lambda \in L$ we have that

$$\langle \mu m, \lambda m \rangle_A = \mathrm{Trace}(\kappa\mu\lambda/g'(\beta)).$$

Since $f_0 \neq 0$, we see that $\kappa \in L^\times$. Define $\alpha = \kappa^{-1} \in L^\times$. Then

$$\langle \mu m, \lambda m \rangle_A = \mathrm{Trace}((\mu\lambda/\alpha)g'(\beta)).$$

By a result from [27, Ch. III, §6], for every $\mu, \lambda \in L$ the value $\langle \mu m, \lambda m \rangle_A$ is the coefficient of β^{n-1} in the expansion of $\mu\lambda/\alpha$ with respect to the basis. Therefore, $\langle \mu m, \lambda m \rangle_B$ is the coefficient of β^{n-1} in the expansion of $\beta\mu\lambda/\alpha$ with respect to the basis.

Define $t \in k^\times$ by

$$t(m \wedge \beta m \wedge \beta^2 m \wedge ... \wedge \beta^{n-1} m) = e \in \wedge^n(W).$$

Then we calculate

$$\langle e, e \rangle_n = t^2 \det(\langle \beta^i m, \beta^j m \rangle_A).$$

Now,

$$\langle e, e \rangle_n = (-1)^{n(n-1)/2} f_0 \text{ and } \det(\langle \beta^i m, \beta^j m \rangle_A) = (-1)^{n(n-1)/2} N(\alpha)^{-1},$$

so $t^2 = f_0 N(\alpha)$.

So far, we have given an étale algebra L corresponding to the binary n-ic form $f(x, y)$. We have also explained how elements $\alpha \in L^\times$ and $t \in k^\times$ satisfying $t^2 = f_0 N(\alpha)$ correspond to the vector (A, B). In defining α and t, we needed to choose a basis vector m for W over L. If we had instead chosen $m' = cm$ with $c \in L^\times$, we would have obtained $\alpha = c^2\alpha'$ and $t = N(c)t'$, so the vector (A, B) only determines the pair (α, t) up to the equivalence relation we described earlier.

It will follow that orbits with invariant $f(x, y)$ exist if and only if $f_0 \in N(L^\times)k^{\times 2}$. If n is odd, the pair $(\alpha, t) = (f_0, f_0^{(n+1)/2})$ will produce an orbit. If n is even, there may be no orbits. For example, when $n = 2$, there do not exist orbits over $\mathbb{R}$ with invariant $f(x, y) = -x^2 - y^2$.

Every equivalence class (α, t) determines an orbit. Since L is n-dimensional over k and W is also n-dimensional over k, there exists a linear isomorphism $\theta : L \to W$ that maps $1 \wedge \beta \wedge ...\beta^{n-1} \in \wedge^n(L)$ to $t^{-1}e \in \wedge^n(V)$. Every other isomorphism that maps these two elements to each other is of the form $h\theta$ for $h \in \mathrm{SL}(W)$. With θ, we can define bilinear forms

$$\langle \theta(\mu), \theta(\lambda) \rangle_A = \mathrm{Trace}(\mu\lambda/(\alpha g'(\beta))) \text{ and}$$

$$\langle \theta(\mu), \theta(\lambda) \rangle_B = \mathrm{Trace}(\beta\mu\lambda/(\alpha g'(\beta)))$$

on W. The $G(k)$-orbit of (A, B) in $V(k)$ is well-defined and has invariant polynomial $f(x, y)$.

Next, we need to figure out what the stabilizer of $(A, B) \in V(k^s)$ is in an orbit corresponding to the binary form $f(x, y)$. To this end, let $L^s = k^s[x]/(g(x))$ be a k^s-algebra of degree n. Since $\langle \cdot, \cdot \rangle_A$ is non-degenerate, the stabilizer of A in G is the special orthogonal group $\mathrm{SO}(W, A)$. Similarly, the stabilizer of B in $\mathrm{SO}(W, A)$ is the subgroup of elements g that commute with T. Since T is regular and semisimple, we find that the centralizer of T in $\mathrm{GL}(W)$ is $k^s[T]^\times = (L^s)^\times$, and every operator in $(L^s)^\times$ is self-adjoint. It follows that the intersection

$$(L^s)^\times \cap \mathrm{SO}(W, A)(k^s)$$

consists of those $g \in (L^s)^\times$ that are self-adjoint and orthogonal, i.e., those g satifying $g^2 = 1$ and $N(g) = 1$. For any k^s-algebra E we can make a similar argument, from which it follows that the elements in $G(E)$ that stabilize (A, B) are precisely those $h \in (E \otimes L^s)^\times$ such that $h^2 = 1$ and $N(h) = 1$. Thus letting $G_{A,B}$ denote the stabilizer of (A, B), we have

$$G_{A,B} \simeq (\mathrm{Res}_{L^s/k^s}(\mu_2))_{N=1}$$

over k^s.

Finally, we need to show that these group schemes descend to $(\mathrm{Res}_{L/k}(\mu_2))_{N=1}$. Since both schemes are flat, we construct isomorphisms and apply faithfully flat descent. The isomorphisms are given by

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

and are compatible with the descent data for each $v \in V_f(k^s)$, i.e., satisfy (2) and (3). Let $\alpha_1, ..., \alpha_n \in k^s$ be the roots of $g(x)$. For each $i = 1, ..., n$, define

$$h_i(x) = \frac{g(x)}{x - \alpha_i} \text{and } g_i(x) = 1 - 2\frac{h_i(x)}{h_i(\alpha_i)}.$$

Suppose $v = (A, B) \in V_f(k^s)$ and $(m_1, ..., m_n)$ is an n-tuple of 0's and 1's such that $\sum m_i$ is even. Let $T = A^{-1}B$ as before. Then we set

$$\iota_v(m_1, ..., m_n) = \prod_{i=1}^{n} g_i(T)^{m_i}.$$

Given a linear operator T on W with characteristic polynomial $g(x)$, $g_i(T)$ acts as multiplication by -1 on the α_i-eigenspace of T and acts trivially on every other eigenspace. This implies that ι_v is injective. Surjectivity follows because $G_v(k^s)$ has the same cardinality as $(\mathrm{Res}_{L/k}(\mu_2))_{N=1}(k^s)$, and a short calculation shows that Equations (2) and (3) are satisfied. □

We now interpret this result cohomologically. To do so, we have to study the cohomology of certain finite group schemes. Let $n \geq 1$ be an integer. Consider the action of S_n on the vector space $N = (\mathbb{Z}/2\mathbb{Z})^n$ by permuting the elements e_i of its natural basis. The non-degenerate

symmetric bilinear form

$$\langle n, m\rangle = \sum n_i m_i$$

is invariant under this action.

Now, let L be an étale k-algebra of rank n, and let $R = \mathrm{Res}_{L/k}(\mu_2)$. Let k^s be a separable closure of k. The absolute Galois group $\mathrm{Gal}(k^s/k)$ acts by permuting the n different homomorphisms $L \to k^s$. This gives a homomorphism $\mathrm{Gal}(k^s/k) \to S_n$ up to conjugacy. We also have an isomorphism $R(k^s) \simeq N$ of $\mathrm{Gal}(k^s/k)$-modules. Letting β be the image of x in $L = k[x]/(g(x)) = k[\beta]$ with $g(x)$ monic and separable of degree n, we see that the n distinct homomoprhisms are obtained by mapping β to the n distinct roots β_i of $g(x)$. Therefore, the points of R over any field extension K of k are in bijection with the monic factors $h(x)$ of $g(x)$ over K.

Let $R_0 = (\mathrm{Res}_{L/k}(\mu_2))_{N=1}$ be the subgroup scheme of norm 1 elements of μ_2. The isomorphism above sends $R_0(k^s)$ to N_0. The points of R_0 over a field extension K correspond to monic factors $h(x)$ of $g(x)$ of even degree over K.

There is a diagonal embedding $\mu_2 \to R$ corresponding to the trivial Galois submodule M of N. The points of R/μ_2 over K likewise correspond to monic factorizations $g(x) = h(x)j(x)$ such that either $h(x)$ and $j(x)$ have coefficients in K or they have conjugate coefficients in some quadratic extension of K. Such factorizations are said to be *rational over* K. For even n, μ_2 is a subgroup of R_0. The points of R_0/μ_2 over K then correspond to even degree monic factorizations $g(x) = h(x)j(x)$ rational over K.

We now wish to calculate the Galois cohomology of these group schemes. Let $R = \mathrm{Res}_{L/k}(\mu_2)$. Then

$$H^0(k, R) = L^\times[2], H^1(k, R) = L^\times/L^{\times 2}, H^2(k, R) = \mathrm{Br}(L)[2],$$

where $\mathrm{Br}(L)[2]$ denotes the 2-torsion subgroup of the Brauer group of L. Let $R_0 = (\mathrm{Res}_{L/k}(\mu_2))_{N=1}$. Then

$$H^0(k, R_0) = L^\times[2]_{N=1}.$$

Moreover, by the long exact sequence in cohomology, we obtain the exact sequence

$$1 \to \langle\pm 1\rangle/N(L^\times[2]) \to H^1(k, R_0) \to L^\times/L^{\times 2} \to k^\times/k^{\times 2} \to H^2(k, R_0) \to \mathrm{Br}(L)[2].$$

The map $H^1(k, R_0) \to L^\times/L^{\times 2}$ induces a surjection $H^1(k, R_0) \twoheadrightarrow (L^\times/L^{\times 2})_{N\equiv 1}$, where $(L^\times/L^{\times 2})_{N\equiv 1}$ denotes the subgroup of $L^\times/L^{\times 2}$ consisting of elemenets with square norm to $k^\times/k^{\times 2}$. The kernel

$$\ker(H^1(k, R_0) \to L^\times/L^{\times 2}) = \mathrm{im}(\langle\pm 1\rangle/N(L^\times[2]) \to H^1(k, R_0))$$

has order one if -1 is the norm of an element of $L^\times[2]$, i.e., if $g(x)$ has a factor of odd degree. Otherwise, the kernel has order two.

Now, if $f \in (V /\!\!/ G)(k)$ is given by

$$f(x,y) = f_0 x^n + ... + f_n y^n$$

with $f(x,1) = f_0 g(x)$, and if $f_0 \neq 0$ and $\Delta(f) \neq 0$, then the stabilizer G_f satisfies $G_f \simeq R_0 = (\mathrm{Res}_{L/k}(\mu_2))_{N=1}$. Moreover,

$$\ker(H^2(k, R_0) \to H^2(k, R)) \simeq k^\times/(N(L^\times)k^{\times 2}).$$

Note that this agrees with Theorem 4.13's statement about orbits with invariant $f(x,y)$ existing if and only if $f_0 \in N(L^\times)k^{\times 2}$.

We claim, but do not prove, that, under this isomorphism, the class of $f_0 \in k^\times/(N(L^\times)k^{\times 2})$ is the class $d_f \in H^2(k, R_0)$ defined earlier. This follows from Theorem 9 of [2]. Since $H^1(k, \mathrm{SL}_n) = 0$ by Theorem 2.21, the only obstruction to the existence of an $\mathrm{SL}_n(k)$-orbit with invariant form $f(x,y)$ is the non-vanishing of d_f. When d_f vanishes, the $\mathrm{SL}_n(k)$-orbits with rational invariant f form a *torsor* for $H^1(k, R_0)$, i.e., they are equipped with a transitive action of $H^1(k, R_0)$ such that the stabilizer of every point under the action is trivial.

5 A few examples of AIT over $\mathbb{Z}$

The original AIT papers [1] and [2] already considered the possibility of applying arithmetic invariant theory not only over fields, but over rings. The ring $\mathbb{Z}$ is particularly useful for the number-theoretic applications of AIT that inspired those two papers, so the examples in the original AIT papers dealt with AIT over $\mathbb{Z}$. Because the methods used in those examples were largely ad hoc, we refer to them as examples of "classical" AIT over $\mathbb{Z}$.

Later, in the preprint [3], the authors observed that a generalized version of the fundamental principle of AIT (i.e., Lemma 3.1) follows basically from a long exact sequence in non-abelian group cohomology. Using this principle, the authors are able to obtain some results over $\mathbb{Z}$. We conclude with a few examples.

5.1 AIT over $\mathbb{Z}$ via long exact sequences

In [3], the authors observe that Proposition 3.2.2 from [14] gives an analogue of Lemma 3.1 for arbitrary schemes. We now state but do not prove this result. It basically follows from standard results about the long exact sequence in non-abelian group cohomology, given in §3 of [14].

Proposition 5.1. *[14], [3] Let G be a group scheme over a base scheme S. Let H be a subgroup scheme of G, and let $X = G/H$, which we take a priori to be a sheaf quotient, i.e., the sheafification of the presheaf defined by $X(U) = G(U)/H(U)$. Then there is a functorial long exact sequence of pointed sets*

$$0 \to H(S) \to G(S) \to X(S) \to H^1(S, H) \to H^1(S, G).$$

We specify more precisely what exactness means for this sequence. We mean that (i) $H(S) \to G(S)$ is injective and the non-empty fibres of the map of sets $G(S) \to X(S)$ are $H(S)$-orbits of $G(S)$, (ii) the images of elements of $X(S)$ are identified in $H^1(S, H)$ if and only if the elements are the same modulo the action of $G(S)$, and (iii) an element of $H^1(S, H)$ is sent to the trivial element of $H^1(S, G)$ if and only if it is in the image of $X(S)$.

Corollary 5.2. *[3] Let G/S be a group scheme over a base scheme acting on a representation V over S. Let $v \in V(S)$. Let G_v denote the stabilizer of G at v. Then there is a functorial long exact sequence*

$$0 \to G_v(S) \to G(S) \xrightarrow{g \mapsto g(v)} (G/G_v)(S) \to H^1(S, G_v) \to H^1(S, G).$$

In particular, if G_v is commutative, then

$$(G/G_v)(S)/G(S) \simeq \ker(H^1(S, G_v) \to H^1(S, G)).$$

Proof. Take $H = G_v$ in Proposition 5.1. □

Remark 5.3. As mentioned in the statement of Proposition 5.1, in general we simply take the quotient $X = G/H$ to be a sheaf quotient. However, in general we have more structure available to us. When H is flat, as is generically the case, then G/H can be equipped with the structure of an *algebraic space*, a slight generalization of a scheme that we will not define. The result holds with any choice of topology: Zariski, étale, fppf, fpqc, Nisnevich, etc.

Remark 5.4. The term $(G/G_v)(S)$ can be thought of as the set of $v' \in V(S)$ that are in the same $G(S')$-orbit as v for some cover $S' \to S$. Then $(G/G_v)(S)/G(S)$ consists of $G(S)$-equivalence classes of such v'.

5.2 Examples

Throughout this section, we use Corollary 5.2 in conjunction with Remark 5.4 to parametrize $\mathbb{Z}$-orbits of representations of various reductive group schemes.

Example 5.5. Let $G = \mathrm{GL}_2$ over $\mathbb{Z}$ act on the representation V of 2×2 matrices. Fix an element $v \in V(\mathbb{Z})$ with characteristic polynomial $x^2 + d$ where $\pm d$ is not a perfect square. Over $\mathbb{Q}$, all such elements are equivalent under the $G(\mathbb{Q})$-action, but we will show this is not the case over $\mathbb{Z}$. The quadratic order O corresponding to such an element is isomorphic to $\mathbb{Z}[x]/(x^2 + d) \simeq \mathbb{Z}[\sqrt{-d}]$. The stabilizer at v is then $G_v \simeq \mathrm{Res}_{\mathbb{Z}[\sqrt{-d}]/\mathbb{Z}}(\mathbb{G}_m)$.

Note that $H^1_{\text{ét}}(\mathbb{Z}, \mathrm{GL}_2)$ vanishes by [3]. Therefore, the $G(\mathbb{Z})$-orbits are in correspondence with the elements of $H^1_{\text{ét}}(\mathbb{Z}, \mathrm{Res}_{\mathbb{Z}[\sqrt{-d}]/\mathbb{Z}}(\mathbb{G}_m))$. By an argument from [3], if O is any quadratic order corresponding to some element $v \in V(\mathbb{Z})$,

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

When $d = 5$, the corresponding quadratic order is (up to isomorphism) $\mathbb{Z}[\sqrt{-5}]$. Then $|\mathrm{Pic}(\mathbb{Z}(\sqrt{-5}))| = 2$, so matrices with characteristic polynomial $x^2 + 5$ fall into two $\mathrm{GL}_2(\mathbb{Z})$-

orbits.

When $d = 1$, the corresponding quadratic order is $\mathbb{Z}[i]$, so since $|\mathrm{Pic}(\mathbb{Z}[i])| = 1$, matrices with characteristic polynomial $x^2 + 1$ fall into one $\mathrm{GL}_2(\mathbb{Z})$-orbit.

Finally, when $d = 3$, $|\mathrm{Pic}(\mathbb{Z}[\sqrt{-3}])| = 2$, so matrices with characteristic polynomial $x^2 + 3$ fall into two $\mathrm{GL}_2(\mathbb{Z})$-orbits. Notice that even though the class number of $\mathbb{Q}(\sqrt{-3})$ is 1, the order $\mathbb{Z}[\sqrt{-3}]$ is not the ring of integers $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ of $\mathbb{Q}(\sqrt{-3})$, which is why we get two orbits rather than one.

We now do the same calculations by hand to illustrate the advantages of the cohomological approach. Any 2×2 integer matrix with characteristic polynomial $x^2 + d$, where $\pm d$ is not a square, has the form

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

and satisfies $a^2 + bc = -d$. The group $\mathrm{GL}_2(\mathbb{Z})$ is generated by the three matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We calculate

$$SAS^{-1} = \begin{pmatrix} -a & -c \\ -b & a \end{pmatrix},$$

$$TAT^{-1} = \begin{pmatrix} a - b & b \\ 2a - b + c & -a + b \end{pmatrix},$$

$$UAU^{-1} = \begin{pmatrix} a & -b \\ -c & -a \end{pmatrix}.$$

Thus, applying S and U in that order, we can assume that $b > 0$, $c < 0$, and $b \leq -c$. Repeatedly applying T or T^{-1}, we can make $|a| \leq \frac{b}{2}$. If at some point we find that $|c| < |b|$, we can apply S and U again to make $b \leq -c$ and continue applying T and T^{-1}. We stop when $|a| \leq \frac{b}{2}$, $b > 0$, $c < 0$, and $b \leq -c$. But then

$$b \leq -c = \frac{a^2 + d}{b} \leq \frac{b}{2} + \frac{d}{b},$$

so $b^2 \leq 2d$.

Now, if $d = 5$ (the x^2+5 case), then $b \in \{1, 2, 3\}$. If $b = 1$, we must have $(a, b, c) = (0, 1, -5)$. If $b = 2$, then $(a, b, c) \in \{(1, 2, -3), (-1, 2, -3)\}$, and these two triples are equivalent under the action of T. If $b = 3$, then $(a, b, c) \in \{(0, 3, -1), (1, 3, -2)\}$, neither of which satisfies $b \leq -c$. A direct calculation shows that the 2×2 matrices corresponding to the triples $(a, b, c) = (0, 1, -5)$ and $(1, 2, -3)$ are not $\mathrm{GL}_2(\mathbb{Z})$-conjugate.

If $d = 1$, then $(a, b, c) = (0, 1, -1)$, so we only get one $\mathrm{GL}_2(\mathbb{Z})$-orbit.

If $d = 3$, then $b \in \{1, 2\}$. If $b = 1$, then $(a, b, c) = (0, 1, -3)$, and if $b = 2$, then $(a, b, c) = (1, 2, -2)$. This once again gives two $\mathrm{GL}_2(\mathbb{Z})$-orbits. We thus recover the results we obtained cohomologically.

Example 5.6. [3], [35] Let $G = \mathrm{GL}_1 \times \mathrm{GL}_2$ over $\mathrm{Spec}(\mathbb{Z})$ act on the representation V of non-zero binary quadratic forms by having GL_1 act by scaling and GL_2 act by its standard action on $\mathbb{A}^2_{\mathbb{Z}}$. Since $0 \neq V$, $V(\mathbb{Z})$ contains only primitive forms (i.e., those with relatively prime coefficients). Let $v \in V(\mathbb{Z})$, and let $\Delta(v)$ denote its discriminant. Since $H^1_{\text{ét}}(\mathbb{Z}, G)$ vanishes by [3], integral equivalence classes of primitive binary quadratic forms with discriminant $\Delta(v)$ are in bijection with elements of $H^1_{\text{ét}}(\mathbb{Z}, G_v)$, where G_v denotes the stabilizer. By §2 of [31], $G_v = \mathrm{Res}_{O/\mathbb{Z}}(\mathbb{G}_m)$ where O is the quadratic order of discriminant $\Delta(v)$. By [3],

$$H^1_{\text{ét}}(\mathbb{Z}, G_v) = \mathrm{Pic}(O).$$

Therefore, $G(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms with discriminant $\Delta(v)$ are in bijection with elements of $\mathrm{Pic}(O)$ where O is the quadratic order of discriminant $\Delta(v)$. This recovers the classical correspondence known as *Gauss composition* over $\mathbb{Z}$.

However, this example is quite similar to our previous one, so now we will make it more interesting by doing it over an arbitrary base scheme. In doing so, we will demonstrate a limitation of AIT over arbitrary schemes.

In [35], Wood observes that the GL_1-action on binary quadratic forms can be viewed, instead of as a scaling, as an invertible change of coordinates. Indeed, given a form $f(x, y) = ax^2 + bxy + cy^2$, we can instead consider the modified form $g(x, y, z) = ax^2z + bxyz + cy^2z$ and then view the $\mathrm{GL}_1(\mathbb{Z})$-action (which is just multiplication by ± 1) as an invertible change of coordinates in the z-variable. Motivated by this observation, Wood notes that the correct generalization of the action of $\mathrm{GL}_2 \times \mathrm{GL}_1$ on the space $\mathrm{Sym}^2(\mathbb{A}^2_{\mathbb{Z}}) - \{0\}$ of non-zero binary quadratic forms is the following.

Let S be an arbitrary base scheme, and let W be a rank 2 vector bundle over S. Let $G = \mathrm{GL}(W) \times \mathrm{GL}_1$ act on $V = \mathrm{Sym}^2(W) \otimes L - \{0\}$, where GL_1 acts on L and the $\mathrm{GL}(W)$ action on $\mathrm{Sym}^2(W)$ is induced by the standard action on $\mathrm{Sym}^2(W)$. In §2 of [35], Wood gives a construction of an O_S-algebra, denoted C, that is analogous to the quadratic order in Gauss composition over $\mathbb{Z}$. (In fact, $C = O_S \otimes \wedge^2(W^*) \otimes L^*$, equipped with a certain algebra structure, but this will not be important for our purposes.)

Let $S' = \mathrm{Spec}(C)$. Then, letting G_v denote the stabilizer of $v \in V(S)$, we wish to calculate $\ker(H^1_{\text{ét}}(S, G_v) \to H^1_{\text{ét}}(S, G))$. By analogy, we would hope that the stabilizer G_v is isomorphic to $\mathrm{Res}_{S'/S}(\mathbb{G}_m)$, but this might only be the case locally. Also, $H^1_{\text{ét}}(S, G)$ might not vanish. We do not know a way of calculating these cohomology groups directly. However, it follows from the main theorem of [35], which was obtained by other methods, that we do actually have $H^1_{\text{ét}}(S, G_v) \simeq H^1_{\text{ét}}(S, \mathrm{Res}_{S'/S}(\mathbb{G}_m))$.

6 Appendix: Non-abelian second Galois cohomology

To the best of our knowledge, no text thus far published on AIT contains a summary of how the second non-abelian Galois cohomology set is defined. The definition of this set is, however, potentially very useful because it allows for the calculation of cohomological obstructions of the type discussed in [2] even in the case where the stabilizers of the algebraic group being considered are non-abelian. (They are always assumed to be abelian in that paper.)

The original description of the second non-abelian Galois cohomology set is in terms of gerbes. That definition, due to Grothendieck, Dedecker, and Giraud, is given in [14]. We discuss a different but equivalent definition first given by Springer in [29]. All definitions in this section can be found in [12].

Definition 6.1. Let k be a field with separable closure k^s. Let $\Gamma = \mathrm{Gal}(k^s/k)$ be its absolute Galois group. Fix $\sigma \in \Gamma$. Let σ^* denote the morphism $\mathrm{Spec}(k^s) \to \mathrm{Spec}(k^s)$ induced by σ. Let G be an algebraic group over k^s, viewed as a group scheme. Let G^σ denote the base change of G by σ^*. Then, letting $p : G \to \mathrm{Spec}(k^s)$ be the structure morphism of G, we have a commutative diagram

$$\begin{array}{ccc} G & \longrightarrow & G^\sigma \\ \downarrow{\scriptstyle p} & & \downarrow \\ \mathrm{Spec}(k^s) & \xrightarrow{\sigma^*} & \mathrm{Spec}(k^s) \end{array}$$

A *σ-semilinear automorphism* of G is an isomorphism of algebraic groups from G^σ to G. A *k-semilinear automorphism* of G is a σ-semilinear automorphism of G for some $\sigma \in \Gamma$.

The k-semilinear automorphisms of G form a group, denoted $\mathrm{SAut}(G/k)$, under composition. We have an exact sequence

$$1 \to \mathrm{Aut}(G) \to \mathrm{SAut}(G/k) \to \Gamma, \tag{4}$$

where the middle arrow is obtained by observing that any automorphism of G is a 1-semilinear automorphism, and the last arrow is obtained by sending σ-semilinear automorphisms to $\sigma \in \Gamma$. Let $\mathrm{Int}(G)$ be the normal subgroup of inner automorphisms in $\mathrm{Aut}(G)$. Define

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G) \text{ and } \mathrm{SOut}(G/k) = \mathrm{SAut}(G/k)/\mathrm{Inn}(G).$$

Taking (4) modulo $\mathrm{Inn}(G)$, we obtain the new exact sequence

$$1 \to \mathrm{Out}(G) \to \mathrm{SOut}(G/k) \to \Gamma. \tag{5}$$

There is an action of $\mathrm{SAut}(G/k)$ on $G(k^s)$, which we now describe. Let $\sigma \in \Gamma$, and let $f_\sigma : G(k^s) \to (G^\sigma)(k^s)$ be the group isomorphism given by

$$f_\sigma(x) = x \circ \sigma^*.$$

Now, given a σ-semilinear automorphism $\phi : G^\sigma \to G$, define the automorphism $\phi_* : G(k^s) \to G(k^s)$ evaluated at $x \in G(k^s)$ by

$$\phi_*(x) = \phi \circ x \circ \sigma^*.$$

Observe that if ϕ' is another σ-semilinear automorphism, then $(\phi\phi')_* = \phi_* \circ \phi'_*$. We have thus defined a homomorphism $\mathrm{SAut}(G/k) \to \mathrm{Aut}\ G(k^s)$. We will often abuse notation by writing ϕ instead of ϕ_*.

We consider $\mathrm{SAut}(G/k)$ equipped with the weak topology with respect to the evaluation maps $\mathrm{ev}_x : \mathrm{SAut}(G/k) \to G(k^s)$ given by $\phi \mapsto \phi(x)$ for $x \in G(k^s)$ and $\phi \in \mathrm{SAut}(G/k)$, i.e., the coarsest topology such that each of these maps is continuous. Here $G(k^s)$ is equipped with the discrete topology.

Definition 6.2. Given a topological space T, a map $T \to \mathrm{SAut}(G/k)$ given by $t \mapsto \phi_t$ is *weakly continuous* if it is continuous with respect to the topology just defined on $\mathrm{SAut}(G/k)$, or equivalently, if for every $x \in G(k^s)$, the map $T \to G(k^s)$ given by $t \mapsto f_t(x)$ is continuous. Note that $t \mapsto f_t(x)$ is continuous if and only if it is locally constant.

Definition 6.3. A *k-form* of G is an algebraic group $\tilde{G}$ over k together with an isomorphism $G \simeq \tilde{G} \times_k k^s$ of algebraic groups over k^s.

Note that given a k-form of G, we obtain a splitting $\Gamma \to \mathrm{SAut}(G/k)$ of (4) given by $\sigma \mapsto \mathrm{id} \times_k (\sigma^{-1})^*$.

Definition 6.4. Let $f : \Gamma \to \mathrm{SAut}(G/k)$ be a section of (4). Let G be an algebraic group over k^s. Let K/k be a finite Galois extension for which there is a K-form $\tilde{G}$ of G. Let $s : \Gamma \to \mathrm{SAut}(G/K)$ be the splitting of (4) associated with $\tilde{G}$. We say f is *continuous* if for every $\sigma \in \Gamma$, the map $\Gamma \to \mathrm{Aut}(G)$ given by

$$\tau \mapsto s_\tau^{-1} f_\sigma^{-1} f_{\sigma\tau}, \tau \in \Gamma,$$

is locally constant.

Definition 6.5. Let G be an algebraic group over k^s. A *k-band in G* is a group homomorphism $\kappa : \Gamma \to \mathrm{SOut}(G/k)$ which splits (5) and lifts to a continuous *map* $f : \Gamma \to \mathrm{SAut}(G/k)$. A *$k$-band* is a pair (G, κ) consisting of an algebraic group G over k^s and a k-band κ in G.

We observe that any k-form $\tilde{G}$ of G defines a splitting of (4) that is continuous, so taking this splitting modulo $\mathrm{Int}(G)$ gives a k-kernel in G. We denote this k-form by $\kappa_{\tilde{G}}$. On the other hand, any continuous splitting of (4) defines a unique k-form of $\tilde{G}$. We do not prove this; it is proved in [6], Lemme 2.12.

Definition 6.6. Let (G, κ) be a k-kernel, and let Z be the centre of G. Then κ induces a k-kernel in Z, i.e., defines a k-form $\tilde{Z}$ of Z. We call $\tilde{Z}$ the *centre* of the k-kernel (G, κ).

For $g \in G$, let $\mathrm{inn}(g)$ denote the inner automorphism induced by g.

Definition 6.7. Let $L = (G, \kappa)$ be a k-kernel. A 2-*cocycle* with coefficients in L is a pair (f, g) of maps

$$f : \Gamma \to \mathrm{SAut}(G/k) \text{ given by } \sigma \mapsto f_\sigma, \text{ and}$$
$$g : \Gamma \times \Gamma \to G(k^s) \text{ given by } (\sigma, \tau) \mapsto g_{\sigma,\tau}$$

such that:

(i) f is continuous as a section;
(ii) $f \bmod \mathrm{Int}(G) = \kappa$;
(iii) $g : (\sigma, \tau) \mapsto g_{\sigma,\tau}$ is continuous (i.e., locally constant); and
(iv) for all $\sigma, \tau, \upsilon \in \Gamma$, we have

$$f_\sigma \circ f_\tau = \mathrm{inn}(g_{\sigma,\tau}) \circ f_{\sigma\tau} \text{ and } f_\sigma(g_{\tau,\upsilon}) \cdot g_{\sigma,\tau\upsilon} = g_{\sigma,\tau} \cdot g_{\sigma\tau,\upsilon}.$$

The set of these 2-cocycles is denoted $Z^2(k, L)$.

We now define an equivalence relation on $Z^2(k, L)$.

Definition 6.8. Two 2-cocycles (f, g) and (f', g') are *equivalent* if there is a continuous (i.e., locally constant) map $h : \Gamma \to G(k^s)$ such that

$$f'_\sigma = \mathrm{inn}(h_\sigma) \circ f_\sigma \text{ and } g'_{\sigma,\tau} = h_\sigma \cdot f_\sigma(h_\tau) \cdot g_{\sigma,\tau} \cdot h_{\sigma\tau}^{-1}$$

for all $\sigma, \tau \in \Gamma$. In this case, we write $(f, g) \sim_{\mathrm{coho},2} (f', g')$. Define the *second cohomology set* $H^2(k, L)$ to be $Z^2(k, L)/\sim_{\mathrm{coho},2}$.

References

[1] Manjul Bhargava and Benedict H. Gross. *Arithmetic invariant theory. Symmetry: Representation Theory and Its Applications; In Honor of Nolan R. Wallach, Progress in Mathematics.* **257**: 33–54 (2014).

[2] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. *Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits. Representations of Reductive Groups; In Honor of the 60th Birthday of David A. Vogan, Jr.* 139–171 (2015).

[3] Anton Geraschenko and David Zureick–Brown (joint work with Asher Auel). *Integral Arithmetic Invariant Theory and Composition Laws.* Preprint (in progress) obtained via personal communication.

[4] Brian Birch. *Cyclotomic Fields and Kummer Extensions.* Published in *Algebraic Number Theory* (edited by J.W.S. Cassels and Albrecht Fröhlich, p. 85–93). *Academic Press.* (1973).

[5] Brian Conrad. *Reductive Group Schemes. Société mathématique de France.* (2014).

[6] Armand Borel and Jean-Pierre Serre. *Théorèmes de finitude en cohomologie galoisienne. Comment. Math. Helv.* **39**: 111–164 (1964).

[7] Nicolas Bourbaki. *Groupes et algèbres de Lie. Hermann.* (1982).

[8] Pete L. Clark. *Quadratic Forms Chapter I: Witt's Theory.* Available at `http://math.uga.edu/~pete/quadraticforms.pdf`.

[9] Cyril Demarche and Giancarlo Lucchini Arteche. *Le principe de Hasse pour les espaces homogènes: réduction au cas des stabilisateurs finis.* To appear in *Compositio Mathematica.* (2019).

[10] Jean A. Dieudonné and James B. Carrell. *Invariant Theory, Old and New. Advances in Mathematics.* **4** (1): 1–80 (1970).

[11] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry.* Latest version available at `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf` (Nov. 18, 2017).

[12] Yuval Z. Flicker, Claus Scheiderer, and R. Sujatha. *Grothendieck's Theorem on Non-abelian H^2 and Local-Global Principles. Journal of the AMS.* **11** (3): 731–750 (1998).

[13] Skip Garibaldi. *Cohomological Invariants: Exceptional Groups and Spin Groups. Memoirs of the AMS.* **200** (937): (2009).

[14] Jean Giraud. *Cohomologie non-abélienne. Springer.* (1971).

[15] David Hilbert. *Ueber die Theorie der algebraischen Formen. Mathematische Annalen.* **36** (4): 473–534 (1890).

[16] Barry Mazur. *Notes on Étale Cohomology of Number Fields. Ann. scient. Éc. Norm. Sup.* **4** (6): 521–556 (1973).

[17] John Milnor and Dale Husemoller. *Symmetric Bilinear Forms. Springer* (1973).

[18] J.S. Milne. *Algebraic Groups.* Avaialble at `https://www.jmilne.org/math/CourseNotes/iAG200.pdf` (2017).

[19] J.S. Milne. *Basic Theory of Affine Group Schemes.* Available at `https://www.jmilne.org/math/CourseNotes/AGS.pdf` (2012).

[20] J.S. Milne. *Reductive Groups.* Available at `https://www.jmilne.org/math/CourseNotes/RG.pdf` (2017).

[21] J.S. Milne. *Arithmetic Duality Theorems.* Available at `http://math.stanford.edu/~conrad/BSDseminar/refs/MilneADT.pdf` (2006).

[22] J.S. Milne. *Lectures on Étale Cohomology.* Available at `https://www.jmilne.org/math/CourseNotes/LEC210.pdf` (2008).

[23] J.S. Milne. *Étale Cohomology. Princeton University Press.* (1980).

[24] David Mumford. *Geometric Invariant Theory, 3rd Ed. Springer.* (1994).

[25] nLab authors. *Galois module.* Available at `https://ncatlab.org/nlab/show/Galois+module` (Revision 8, 2019).

[26] Jean-Pierre Serre. *Galois Cohomology. Springer.* (1997).

[27] Jean-Pierre Serre. *Local Fields. Springer.* (1979).

[28] Pierre Deligne (with the collaboration of J.F. Boutot, A. Grothendieck, L. Illusie, and J.L. Verdier). *Séminaire de Géométrie Algébrique du Bois-Marie: Cohomologie Étale (SGA* $4\frac{1}{2}$*). Springer.* (1977).

[29] T.A. Springer. *Nonabelian* H^2 *in Galois cohomology. Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965.* 164–182 (1966).

[30] The Stacks project authors. *The Stacks Project.* Available at `https://stacks.math.columbia.edu`. (2019).

[31] Takashi Taniguchi. *On proportional constants of the mean value of class numbers of quadratic extensions. Trans. Amer. Math. Soc.* **359** (11): 5517–5524 (2007).

[32] Ravi Vakil and Kirsten Wickelgren. *Universal covering spaces and fundamental groups in algebraic geometry as schemes. Journal de Théorie des Nombres de Bordeaux.* **23** (2): 489–526 (2011). Available at `http://www.numdam.org/article/JTNB_2011__23_2_489_0.pdf`.

[33] William C. Waterhouse. *Introduction to Affine Group Schemes. Springer.* (1979).

[34] Hermann Weyl. *Invariants. Duke Math Journal.* **5** (3): 489–502 (1939).

[35] Melanie Matchett Wood. *Gauss composition over an arbitrary base. Adv. Math.* **226** (2): 1756–1771 (2011).

[36] Wouter Zomervrucht. *Faithfully Flat Descent.* Available at `http://www.math.leidenuniv.nl/~wzomervr/docs/ffdesc.pdf` (2013).